



Privacy Impact Assessment for Call Centre Software TC3 Upgrade

PIA#SBRT17001

Part 1 – General

Name of Ministry:	Small Business and Red Tape Reduction / Liquor Distribution Branch		
PIA Drafter:	Manami Calvo		
Email:	Manami.Calvo@bcldb.com	Phone:	604-252-3011
Program Manager:	Erin McEwan		
Email:	Erin.McEwan@bcldb.com	Phone:	604 252-3479

1. Description of the Initiative

The LDB is upgrading its Call Centre software. Currently the LDB's current Call Centre software is called "Call Centre Anywhere" or CCA. It is used in the two Call Centres that LDB operates:

- The LDB's Vancouver Wholesale Customer Centre at the LDB's Head Office at 3200 East Broadway (software going live March 2017)
- The LDB's Support Centre at 3200 East Broadway, Vancouver (software going live in February 2017)

Call Centre agents in these two locations are called "CCA agents" or "TC3 agents".

The LDB's Wholesale Customer Centre clientele consists of the 7000 wholesale liquor customers (i.e. owners of hospitality establishments such as pubs and restaurants) who call the centre for assistance with ordering, questions regarding the Wholesale Customer online catalogue, etc.

The LDB's Support Centre clientele consists of internal (i.e. LDB Head Office employees and BC Liquor Store employees) calling for IT assistance as well as external customers, calling for assistance with the LDB's outward facing applications such as the Special Occasion License online application form.

Please note that the LDB Support Centre is open Sunday 830am-Friday midnight and Sat 500-midnight. The LDB Wholesale Customer Centre is open from 8am-4pm Mon-Friday. When a CCA/TC3 Agent is available to answer the phone the personal information of the caller is not collected as CCA/TC3 agents are instructed NOT to record any personal information as part of their training. They may give instructions or advice but they do not record any names or contact information of callers. If an issue needs to be escalated to a WCC supervisor the CCA/TC3 agent will transfer the call to the supervisor on duty.

Since 2009 the LDB has contracted with Telus Communications Inc. (TELUS) for the CCA solution. This contract is separate from the Telus' contract with the Province (MTICS). This software is

For PCTB Use Only:

Version 1.0

1



Privacy Impact Assessment for *Call Centre Software TC3 Upgrade* PIA#SBRT17001

current “on premise”, hosted on the LDB’s own servers and the LDB monitors and maintains the application, the hardware, and the Operating System. The services that TELUS provides under the umbrella of the CCA include:

- Phone queuing (i.e. software which places phone calls in the order they are made)
- Answering service (software that provides voicemail to CCA / TC3 agents)
- Voicemail
- Voicemail to email conversion (i.e. voicemail messages are converted to an email message and sent to a designated email account accessible by CCA/TC3 Agents, if voicemail not deleted in 23 hours)
- Time and staff tracking / reporting and metrics (please see below metrics):
 - Agent Answered - Inbound/Outbound
 - Agent Answered within Thresholds - 30/60/90 Seconds
 - Abandoned
 - Abandoned within Threshold - 30/60/90 Secs
 - Callbacks
 - Voicemails
 - No Answers
 - Agent Login/Logout
 - Talk Time/Wrap Time/Hold Time/Average Handle Time (AHT)
 - Different Status time (Available Time/Busy Time/Break Time/Last Call)
 - Call Interval Time (15 min interval)
 - Service Level Performance (Daily, Weekly, Monthly - In 15 min intervals)
 - Calls hitting different menus in Call Tree (Internal, External, HO, Stores, etc)
 - Segment Report
 - Interval Report
- Recording of phone calls for performance management and training purposes, which includes:
 - WCC and Support Centre Supervisors and/or Managers proactively monitors calls and rates them against our call quality guidelines to ensure we provide consistent level of service.
 - WCC and Support Centre Supervisors and/or Managers use the calls during refresher training and new hire training.
 - WCC and Support Centre Supervisors and/or Managers - Pinpoint deficits and proficiencies in agent performance
 - WCC and Support Centre Supervisors and/or Managers - We use recordings to improve feedback during coaching sessions
 - WCC and Support Centre Supervisors and/or Managers - Facilitate the goal setting process
 - WCC and Support Centre Supervisors and/or Managers - Track progress
 - WCC and Support Centre Supervisors and/or Managers - Pinpoint agents in need of remediation



Privacy Impact Assessment for *Call Centre Software TC3 Upgrade* PIA#SBRT17001

- WCC and Support Centre Supervisors and/or Managers - Expedite agent skill-building, training and development
- WCC and Support Centre Supervisors and/or Managers - Improve service quality and customer satisfaction
- WCC and Support Centre Supervisors and/or Managers - We also use call recordings to review interactions for complaint resolutions and verifications.
- For Wholesale Customer Centre only : in Labour Relations processes to hold agents accountable for any inappropriate or incorrect comments given to customers
- Only supervisors and managers have access to these voice recordings. Analysts will hear the call during the one on one coaching session.

The LDB has decided to move its Call Centre Services to a cloud service provider, primarily for cost savings purposes (i.e. labour, OS, Software and hardware costs necessary to host and maintain an LDB-served system). The LDB is looking to upgrade its contract with TELUS so that these same CCA services will be provided on Telus' Cloud Centre called the "Telus Cloud Contact Centre" or TC3 and all services will be stored and maintained on the Telus cloud solution, off premise.

2. Scope of this PIA

This PIA describes a) the services that TELUS currently provides the LDB Call Centres (the LDB's Vancouver Wholesale Customer Centre, and the LDB's Support Centre under its Call Centre Anywhere contract and b) the upcoming changes to these services when CCA is upgraded to Telus' Cloud-Based Solution.

3. Related Privacy Impact Assessments

N/A – the LDB does not have a previous PIA on CCA

4. Elements of Information or Data

Voicemail:

Callers to LDB Call Centres may leave personal information in their voicemail messages (i.e. name and personal phone number so that LDB employees may return their phone call).

Voicemails will be retained for 23 hours (at which point they may be converted to emails, then deleted when responded to).



Privacy Impact Assessment for *Call Centre Software TC3 Upgrade* PIA#SBRT17001

The CCA system also records the phone conversation between the CCA agent and the customer, for training and program improvement purposes.

Performance Management Data:

The CCA system provides information about the performance of call centre agents. The following data is collected from LDB CCA/TC3 Agents and will be used as part of the employees' performance assessment:

- Agent Answered - Inbound/Outbound
- Agent Answered within Thresholds - 30/60/90 Seconds
- Abandoned
- Abandoned within Threshold - 30/60/90 Secs
- Callbacks
- Voicemails
- No Answers
- Agent Login/Logout
- Talk Time/Wrap Time/Hold Time/Average Handle Time (AHT)
- Different Status time (Available Time/Busy Time/Break Time/Last Call)
- Call Interval Time (15 min interval)
- Service Level Performance (Daily, Weekly, Monthly - In 15 min intervals)
- Calls hitting different menus in Call Tree (Internal, External, HO, Stores, etc)
- Segment Report
- Interval Report
- Recording of phone call for performance management and training purposes.

1. It should be noted that our current call center software retains all caller-id numbers, this is an accepted industry-standard for call center software.
2. The phone numbers are retained for 12 months then automatically deleted from the system.
3. We have two valid business reasons for requiring the caller-id:
 - a. We use it to contact the caller
 - b. We use it to review the history of the caller experience, which aids us in training and improvements (i.e. if the same callers calls back frequently, we may look into whether that they are not satisfied with our services or if there is a training gap.. Please note CSA agents will not use Caller ID to call the customer back to review customer experience. Only metrics will be used for training and program improvement purposes

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 unsigned to PCTB at pia.intake@gov.bc.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.



Privacy Impact Assessment for Call Centre Software TC3 Upgrade

PIA#SBRT17001

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

As per the contract with TELUS all Telus Cloud Contact Centre software will be hosted in Canada.

“TELUS Cloud Contact Centre is hosted in our Tier 1 data centres, all Canadian-based to alleviate concerns about the residency of your data”.

Please see “TELUS Cloud Contact Centre (TC3) - Security Posture Document” in Appendix A for more details.

With regards to the services that TELUS currently provides the LDB Call Centres (the LDB’s Vancouver Wholesale Customer Centre and the LDB’s Support Centre under its Call Centre Anywhere contract), the software is “on premise”, hosted on the LDB’s own servers and the LDB monitors and maintains the application, the hardware, and the Operating System.

6. Data-linking Initiative*

In FOIPPA, “data linking” and “data-linking initiative” are strictly defined. Answer the following questions to determine whether your initiative qualifies as a “data-linking initiative” under the Act. If you answer “yes” to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no
If you have answered “yes” to all three questions, please contact a PCTB Privacy Advisor to discuss the requirements of a data-linking initiative.	



Privacy Impact Assessment for Call Centre Software TC3 Upgrade PIA#SBRT17001

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

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

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Individuals telephone the LDB Support Centre and the LDB Wholesale Centre through the publicly available contact information on LDB websites to request information. Their Caller ID (i.e, name and telephone number) are collected and stored through the CCA software and accessible by staff through the telephone queue. so that it can be monitored for training and program improvement purposes (i.e. so that we can track repeat calls from the same customer and determine if customer service is an issue). Phone calls themselves are also recorded for performance management , training and program improvement	Collection Use	26(c)(e) 32(a)



Privacy Impact Assessment for Call Centre Software TC3 Upgrade PIA#SBRT17001

	purposes. When CCA/TC3 Agents are speaking to individuals or employers about general inquiries related to the LDB, they will provide the information or provide an alternate contact (e.g. LCLB)		
2.	Caller leaves a voicemail when all CSA/TC3 agents are busy, with their name and contact information (i.e. phone number), in order to receive a call back.	Collection	26(c)
3.	CSA/TC3 agent use the contact details of customers to respond to the voicemail (i.e. call them back)	Use Disclosure	32(a) 33.1(7)
4.	Voicemail is retained for 23 hours, then converted to email and deleted once the CSA/TC3 agent has responded to the inquiry	Use	32(a)
	Caller ID (name and phone number) is retained for 1 year for performance management, training and program improvement purposes	Use	32(a)
	Phone call recordings are retained for 90 days (and then purged), for performance management, training and program improvement purposes	Use Disclosure	32(a) 33.2(a) or (c)
	Voicemail is retained for 24 hours and then converted to email if the voicemail if it has not been responded to. The email is deleted once it has been responded to).	Use	32(a)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	LDB employees use or disclose the personal contact details of other employees or customers for unauthorized purposes.	Code of Conduct.	Low	Low

For PCTB Use Only:
Version 1.0



Privacy Impact Assessment for Call Centre Software TC3 Upgrade

PIA#SBRT17001

2.	Telus employees or subcontractors could access personal information and use or disclose it for personal purposes.	Security risks will be mitigated by CSA signed by Telus and the LDB.	Low	Low
----	---	--	-----	-----

10. Collection Notice

The below notification played before any CCA agent answers the phone (and not just for calls that go to voicemail). If no one is available then it will go to voicemail after the below notification is played (in other words, the below notification will play with every phone call, whether someone picks up or it goes to voicemail):

Please note this call we will be recorded for training and program improvement purposes

Any personal information that you provide during this call will be collected by the Liquor Distribution Branch under 26 (c) and (e) of the Freedom of Information and Protection of Privacy Act, in order to respond to your request for assistance and for training and program improvement purposes. If you have any concerns please ask the next available representative. If you have further questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5.

LDB Call Centre employees, both at the LDB's Support Centre as well as the Wholesale Customer Centre are told their performance may be tracked through the CSA tool in their training and are told their calls will be recorded for training and program improvement purposes.

The following collection notice will be added given to staff:

Please note that your phone calls with customers will be recorded for performance management, training and program improvement purposes pursuant to section 26 (e) of the Freedom of Information and Protection of Privacy Act. If you have any questions please ask your supervisor. If you have further questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when



Privacy Impact Assessment for *Call Centre Software TC3 Upgrade* PIA#SBRT17001

filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

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

N/A – Public access is only available through Corporate VPN access (section 2.3.2 of TC3 Security Posture Document - TELUS Support Infrastructure Access section in Appendix A).

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

Please see section 2.4 of *TC3 Security Posture Document* (Protection Against External Threats) in Appendix A.

13. Does your branch/department rely on any security policies?

Yes, please see TC3 Security Posture Document in Appendix A.

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

Please see section 2.3 of *TC3 Security Posture Document* (Access Control to the TC3 Service and Supporting Infrastructure) in Appendix A.

Part 4 – Accuracy/Correction/Retention of Personal Information

15. 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 public body notify them of the update, correction or annotation?

Not updated or corrected- voicemail is transitory information, used only to return the customer's call.

It will not be disclosed to others outside the LDB Call Centres.

Caller-id numbers are retained for 12 months, and then automatically deleted from the system.

If an agent would like to request that a change to a call recording be made they can make a request to their supervisor. If the change is not made, there will be a note made that the agent made the request.

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



Privacy Impact Assessment for *Call Centre Software TC3 Upgrade* PIA#SBRT17001

No

17. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

18. If you answered "yes" to question 17, do you have a records retention and/or 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?

N/A

Part 5 – Further Information

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

No

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

No

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

No

Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.



Privacy Impact Assessment for Call Centre Software TC3 Upgrade PIA#SBRT17001

Part 6 – PCTB Comments and Signatures

This PIA is based on a review of the material provided to PCTB as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCTB.

Andrea Fox

March 3, 2017

Privacy Analyst
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Finance

Signature

Date

Quinn Fletcher

April 3, 2017

Senior Privacy and Policy Advisor
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Finance

Signature

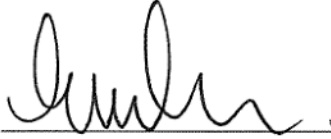
Date



Privacy Impact Assessment for Call Centre Software TC3 Upgrade PIA#SBRT17001

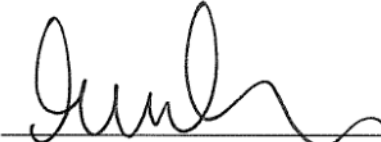
Part 7 – Program Area Comments and Signatures

Erin McEwan,
Director, IT Risk & Support
Services, Information Services


Signature

Apr. 10. 17
Date

Erin McEwan,
Ministry Contact Responsible for
Systems Maintenance and Security


Signature

Apr. 10. 17.

Blain Lawson
CEO and General Manager, LDB


Signature

4/10/2017
Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCTB for its records to complete the process. PCTB is the designated office of primary responsibility for PIAs under ARCS 293-60.

PCTB 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. If you have any questions, please contact your privacy advisor at PCTB or call the Privacy and Access Helpline at 250 356-1851.

Page 013 of 163 to/à Page 025 of 163

Withheld pursuant to/removed as

s.15 ; s.21



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM)

PIA# SBRT17008

Part 1 – General

Name of Department/Branch:	Liquor Distribution Branch , Ministry of Attorney General		
PIA Drafter:	Kenny Chan , Manager, IT Change		
Email:	Kenny.chan@bcldb.com	Phone:	604-252-3070
Program Manager:	Kenny Chan, Manager, IT Change		
Email:	Kenny.chan@bcldb.com	Phone:	604-252-3070

1. Description of the Initiative

This PIA looks at the Liquor Distribution Branch's (LDB) three implementation phases of Marval's Integrated IT Service Management application (MSM) implementation.

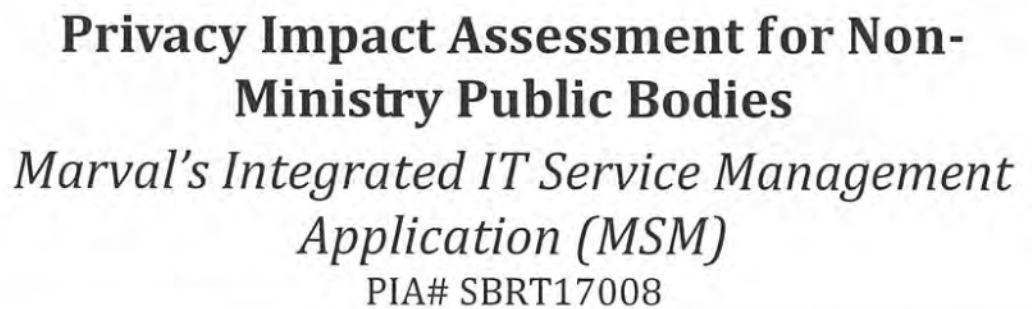
MSM is a ticketing system tracking tool used by our Information Services team, to log and track human resource and information technology related requests and issues raised by LDB employees and customers by phone or email to the Support Centre. LDB employees obtain the Support Centre's phone number and email through the address book in Microsoft Outlook. LDB customers obtain the Support Centre's phone number and email from the Special Event Permit website (<https://specialevents.bcldb.com/contact>) which they will be visiting in order to sign up to obtain a Special Event Permit.

MSM has been implemented in three phases which are described in the following section.

2. Scope of this PIA

The scope of this PIA covers the flow of information through the MSM tool, it does not include the escalation of tickets to another department the three implemented phases of MSM (note that only Phase 2 and 3 includes personal information):

Phase 1 – This phase of MSM was implemented in October 2014 strictly for internal use. The scope of this phase was to replace the LDB's former BMC Software Inc. ticket tracking system with MSM. The BMC software was replaced with MSM to allow for better integration of all service delivery processes, tracking and reporting. Similar to our former tracking system, the LDB Information Services Support Centre team tracks issues reported to them through phone or email from an internal employee (store staff, Head Office staff or Distribution Centre staff) through

[illegible]

2



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

information) may be included in these emails derived from the ticket. However, all Helpdesk staff will be instructed in their training not to record any PI that they received through phone or email from employees asking for assistance with HR-related inquiries, it is expected that only business contact information (i.e. name, and contact) will be involved (i.e. no benefits information, sick leave information).

Phase 3 – This phase of MSM was implemented in June 2015 and is now up and running. This phase involves LDB Support Centre staff receiving requests and queries from customers of BC Liquor Stores (i.e. from the public) regarding technical issues they experience with logging onto the LDB customer online portal to access their Liquor Control Licensing Branch's Special Event Permit application, process for acquiring license, and any other technical issues with public-facing technologies (e.g. website, web services etc.). Support Centre staff will log these requests into MSM. Some personal information (e.g. customer name and contact information and details of the technical issues of customers) may be included in these tickets. However, Support Centre staff is instructed to record the minimum contact information that is necessary to follow up on the ticket.

For clarity, Support Centre staff will receive the standard FOIPPA training that is received by all BCLDB staff on the collection and use of personal information and are instructed in program area training not to collect personal information from customers when addressing user/customer calls from Head Office and stores, and are occasionally reminded of the privacy policy through emails from management.

3. Related Privacy Impact Assessments

- Identify Access Management PIA regarding the LDB customer portal to access (JAG 15038)
- Special Occasion License Online (JAG15001)
- Call Centre Anywhere Software Upgrade (SBRT17001)
- PIA Initiative Update – Identity Access Management - HR Onboarding Process (SBRT 16004)

4. Elements of Information or Data

- Customer/Employee name
- Customer/Employee phone number
- Customer/Employee email address
- Details of inquiry/request
- Potentially employee payroll/benefits/sick-leave information in email

(IP Addresses of customers not collected as the ticket is logged in by LDB staff)



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

There is no storage or access outside of Canada. The MSM is owned by Marval, a Canadian company whose data centres are in Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No

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

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	<u>Phase 2 and 3:</u> Support Centre staff receive an inquiry or request from staff or customer via email or phone call and record the information into the MSM tool	Collection	26(c)&(e)
2.	Support Centre staff may escalate ticket to another LDB department for further investigation as necessary. (Once the ticket is escalated, it is out of scope of this PIA.)	Disclosure	33.2(a), 33.2(c)
3.	Information from inquiry/request is used to resolve the technical issue of the user or assign the ticket to another department.	Use	32(a)



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM)

PIA# SBRT17008

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Third party service provider experiences a breach and customer as well as employee information is accessed unlawfully.	Appendix G (schedule G) forms part of the contract with Marval and personal information is identified and the contractor's obligation to protect the information is stated. A Personal Protection Schedule is also included in the Province's contract with TSSA.	Low	High (in case of sensitive HR information)
2.	There is a risk that LDB employees can look up information in the system that they do not have a business reason to access, i.e. a neighbour's BCM ticket or a work colleague's HR information.	Employees have appropriate access levels; audit trails; Employee Code of Conduct;	Low	Med

10. Collection Notice

In regards to the LDB's Support Centre staff receiving requests and queries from customers of BC Liquor Stores (i.e. from the public) regarding technical issues they experience, limited contact information from customers, for example name, phone number and email address are collected, for the purposes of responding to their inquiries and requests.

Customers are given notice of the collection of their personal information when they call the Support Centre and listen to the below auto message (played before the call is answered):

Any personal information that you provide during this call will be collected by the Liquor Distribution Branch under 26 (c) and (e) of the Freedom of Information and Protection of Privacy Act, in order to respond to your request for assistance and for training and program improvement purposes. If you have any concerns please ask the next available representative. If you have



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM)

PIA# SBRT17008

further questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5.

Customers can view the Privacy Policy on the LDB website when they submit a request via email through the LDB Special Event Permit Contact Us page. The My LDB Account Privacy Notification reads as follows:

In regards to the My LDB Account sign up page, the Liquor Distribution Branch is collecting your personal information to manage your user identity and access permissions for LDB applications. This information is being collected pursuant to section 26(c) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of your personal information please contact Information, Privacy and Access Services, BC Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3043.

Part 3 – Security of Personal Information

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

The MSM System is hosted from a collocation service provided by Cogeco Data Services (CDS) at a data centre in Toronto. CDS' description of the collocation services, which includes a description of physical security controls, for this data centre is annually audited. The 2013 description was audited by Pricewaterhouse Coopers in accordance with CPA and AICPA standards. They concluded that the description of the system and the control design and operations met the control objectives.

The Physical Security Controls include the following:

- Access control devices including a security access system, digital video recorders, proximity cards, and a biometric authorization system have been installed that limit access to the collocation data centre facilities.
- The physical access security systems segregate access to the collocation data centre facilities and other areas. Clearance levels for the areas are determined based on job function.
- Access to collocation data centre facilities is restricted and is appropriately authorized through a formal management approval process.



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

- Sign-in is required for visitors requesting access to the collocation data centre facilities. Visitors who are not CDS pre-approved contractors, CDS customers listed on authorized access list, or CDS employees are required to be escorted by a CDS operations staff. Visitors who are customer contractors are required to be escorted by the contracting customer or a CDS operations staff.
- Customers are assigned access to the rooms in which the cabinets and cages they are authorized to access are located.
- Access is removed the same day for terminated and transferred employees who no longer require access.
- Physical access rights for employees are reviewed quarterly by the Data Centre Manager or a designate and the security access system is updated as necessary.
- Access to the Access Control Management Software (ACMS) controlling card readers is limited to authorized users through user IDs, passwords and limited physical access to the ACMS workstations and servers.
- Physical access activity within the collocation data centre facilities is logged for a period of 90 days.
- CDS maintains anonymity of customers within the data centre facilities. Cabinets/ cages are only designated with generic labels.

CDS recruiting and selection of candidates follows an established HR process which is designated to recruit, develop, and retain competent employees. Personnel requirements include: Hiring Principles, Background Checks, New Hire Orientation, Job Training, Security and Safety Awareness, Non-disclosure Agreements, Employee Performance Management, and Skills Development.

Marval personnel with access to LDB information have been screened and sign a confidentiality agreement.

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

Data center resources are protected by a firewall array (multiple firewalls, multiple paths) that inspect every digital packet and evaluate against rules and known vulnerabilities. The traffic on the wire is placed into zones of security. Each IP address that initiates a connection is tracked and controlled.



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

Access to servers is restricted to a limited list of IP addresses. All protocols are evaluated on whether or not they need to be open to the Internet or a restricted group of computers. IP restrictions will result in the firewall blocking access even to open ports.

The firewalls are aware of each other and they do IPS and IDS services. Ports that are opened to the Internet are monitored and scanned for abuse of the protocol and they are dynamically blocked if DDOS attacks or exploits are detected in the traffic.

Notification messages are sent securely to monitoring personnel and they do not cross the Internet in plain text.

s.15; s.21

13. Does your branch/department rely on any security policies?

We are relying on our own and Marval's security policies.

14. 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.

Access to server resources requires a username and password. Only the support team that is authorized to provide technical support is on the access list that provides access to the server. This list is strictly controlled.

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

All access to resources in the application is logged by the application and viewable by application administrators for auditing purposes. Each application user has a login credential, which is assigned with access permissions necessary for carrying out their duties. When they access resources that are stored in the application, their credentials and time of access is logged automatically by the system.

Breaches when detected follow a three stage process, which is aligned with the BC Government's information security incident process:



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

1. Notification of suspicious activity will occur within an hour of detection. Marval Service Desk will be notified and involved in the investigation. All reported security breaches are considered a high priority incident and a security specialist will move to address the report immediately. Customer notifications will then be sent.
2. Confirmation of a breach will result in a bulletin to all the site contacts informing all parties of the breach and identifying the scope of the risk. Steps to mitigate the breach will be outlined.
3. A post mortem will be conducted and information provided to all parties with details of how the breach occurred, steps to prevent a similar breach and steps to harden security.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. 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 public body notify them of the update, correction or annotation?

Customers or employees can call Support Centre staff and request that their ticket be updated (i.e. providing a new phone number or email).

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

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A.

19. If you answered "yes" to question 17, do you have a records retention and/or 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?

Tickets will be kept in accordance to the ARCS records retention policy (6820-25 – Reported incidents and user help support).



Privacy Impact Assessment for Non-Ministry Public Bodies
Marval's Integrated IT Service Management Application (MSM)
PIA# SBRT17008

Part 5 – Further Information

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

No.

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

No.

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

Each MSM request will be assigned a unique ticket number. Customers are given this ticket numbers so that they can reference it when if call into th eSupport Centre again.

PIB Information:

Personal Information Bank – Required Information	
Description	MSM Tickets
Primary ministry/government agency involved	Ministry of Small Business and Red Tape Reduction/ Liquor Distribution Branch
All other ministries/government agencies and public bodies involved	None
Business contact title	Privacy Officer
Business contact telephone number	604-252-3011



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

Part 6 – PCTB Comments and Signatures

This PIA is based on a review of the material provided to PCTB as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCTB.

Section 69 (5.1) of the Freedom of Information and Protection of Privacy Act (FOIPPA) requires the submission of a Privacy Impact Assessment (PIA) during the development stage of any proposed enactment, system, project, program or activity.

However, due to the fact that both PCT and SBRT understood LDB to be a quasi-independent corporation who were not required to submit PIAs to PCT for review, this PIA was not submitted during the development stage. This is now understood by all parties to have been incorrect and this PIA was submitted to the Privacy, Compliance and Training Branch (PCT) subsequent to the program's start dates. The final phase of the program began in June 2015. The PIA was not submitted to PCT until June 6th, 2017. As such, PCT was unable to provide any meaningful recommendations or advise the program area of any risk-mitigation strategies. No privacy concerns were noted in the review.

PCT looks forward to reviewing future PIAs that are completed and provided to PCT with ample time to provide feedback, as is legislatively required. If you have any questions or concerns, our privacy advisors are available to provide assistance.



Privacy Impact Assessment for Non-Ministry Public Bodies
Marval's Integrated IT Service Management Application (MSM)
PIA# SBRT17008

Chris Reimer

A handwritten signature in black ink, appearing to read "Chris Reimer".

October 12, 2017

Senior Privacy and Policy Analyst
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Finance

Signature

Date

Quinn Fletcher

A handwritten signature in black ink, appearing to read "Quinn Fletcher".

October 23, 2017

Senior Privacy and Policy Advisor
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Finance

Signature

Date



Privacy Impact Assessment for Non-Ministry Public Bodies

Marval's Integrated IT Service Management Application (MSM) PIA# SBRT17008

Part 7 - Program Area Signatures


Kenhy Chan, Manager IT Change

Signature

Nov 10, 2017
Date


Erin McEwan, Director, IT Risk and
Support Services

Date

Nov 3 / 17

Date

Blain Lawson, CEO and General
Manager

Signature



Nov 15, 2017
Date

PRIVACY IMPACT ASSESSMENT

Initiative Update – AG18005

1. Title of original PIA and any number assigned to original PIA

JAG 15038 - Identity and Access Management for BC LDB
SBRT 16015 - LDB Hospitality Customer Identify and Access Management Account initiative PIA Update

2. Ministry/Public Body and Program Area.

Ministry	Ministry of Attorney General
Division	Liquor Distribution Branch (LDB)
Branch/Section	Information Services
Initiative Title	IAM Update – Adding Secondary Users to LDB Hospitality Customers' IAM Accounts

3. Contact Position and/or Name, Telephone Number and E-Mail Address.

Name, Title	Manami Calvo
Branch/Section	Information, Privacy and Access services
Phone Number	604 252-3011
E-Mail	Manami.Calvo@bclldb.com

4. Description of the revision.

Identity access management (IAM) is a LDB's software application that creates and manages user accounts to LDB internal and external facing LDB systems, including authentication and validation of authorization to access the Hospitality Product Catalogue.

In the original 2015 PIA, the use of the LDB's Identity and Access Management (IAM) system was limited to onboarding external users (i.e. member of the public) and internal users (i.e. LDB employees and contractors). The main purposes were to provide the ability for external users to create a "profile" for themselves in IAM (i.e. by registering basic self-identifying information such as a user name, password, contact details) in order to sign in and access approved, external facing Liquor Distribution Branch (LDB) systems (i.e. Special Occasion License Online website – *renamed to Special Event Permit*) and for LDB to create IAM profiles for internal users as part of their new employee onboarding process to allow for a partial sign-on to some internal applications. IAM ensured that access privileges were granted according to a single interpretation of policy and all individuals and services were properly authenticated, authorized and audited.

LDB's Identity and Access Management (IAM) system was subsequently updated to also collect the personal information of new employees in order to establish their Human Resources and Payroll records with the LDB and the BC Public Service Agency and used to authenticate and authorize access to the Hospitality Product Catalogue by LDB's hospitality customers.

IX DMIP OR FOIPP COORDINATOR - REVIEW cont'd

In this PIA update, the following two processes are described:

- The process by which wholesale customers sign up to order liquor products online from LDB's Webstore on-line ordering system
- The process by which wholesale customers can add a secondary user to their IAM account, who can then order liquor product from the LDB's Webstore on-line ordering system on their behalf.

Process by which wholesale customers sign up to order online from LDB's Webstore on-line ordering system:

1. Before being able to sign up for an IAM account wholesale customers must first sign up for a BCeID account to access online government services. BCeID is a separate public body from the LDB and therefore the process of signing up for a BCeID is not documented in this PIA. Please see <https://www.bceid.ca/> for more information regarding signing up for a BCeID account.
2. After setting up a valid BCeID account, LDB Wholesale customers must then register for an LDB IAM account to be able to access and place orders using LDB Webstore. They can register either through an online form or by calling one of the Wholesale Customer Centres (WCCs).

Online registration form:

- 1) To register online wholesale customers must first fill out a registration form online and submit it. The online registration form found at the following link:
<https://wholesale.bcldb.com/register>

The following business information is collected from customers on the online form:

- License Number (i.e. valid license issued by Liquor Control Licensing Branch which authorizes you to purchase liquor from the LDB for the purpose of resale or a rural agency store or a duty free store authorized by the LDB)
- Company Name
- CRA Business Number
- Privacy BCeID
- First Name
- Last Name
- Address
- City
- Postal Code
- Phone
- Email

In the webstore privacy policy it is stated that all information collected for webstore registration is considered business contact information and not personal information:

IX DMIP OR FOIPP COORDINATOR - REVIEW cont'd

https://wholesale.bcldb.com/sites/default/files/files/2017-09/Web%20Store%20Terms%20and%20Conditions%20Privacy%20Statement%20Registration_0.pdf

3) Secondly, an LDB IAM administrator from one of the LDB's Wholesale Customer Centres (wholesale customer representative) receives the completed online form that has been submitted electronically. They will log into their IAM administrator account and perform the following steps:

- a) Select "Create User from BCeID".
- b) Enter the BCEID supplied by the Wholesale Customer on the online form. If there is a match the First Name, Last Name and Business Email address are displayed.
- c) They then click "Submit" to add the account to the IAM system
- d) They then click "Manage Wholesale User"
- e) They search for the user entered in steps 2-5 by BCeID or Email address
- f) They enter the users contact information (address, phone number) supplied by the user on the online form.
- g) They add one or more licence number as supplied by the Wholesale Customer.
- h) They click submit again.

4) The LDB IAM administrator from the LDB's Wholesale Customer team sends an email to the Wholesale Customer confirming that their IAM account has been created and that they can login to IAM and order online.

5) The Wholesale Customer logs in to Webstore using their BCeID account and password and orders liquor product for the assigned Licence(s). The link to login to Webstore is available on the LDB's Wholesale website (<https://wholesale.bcldb.com/retailers>), as shown in the screen shot below.

Log in with BCeID

User ID
Use a Business BCeID

Password

Continue

IX DMIP OR FOIPP COORDINATOR - REVIEW cont'd

Registration by phone:

1) To register by phone to order online on webstore the wholesale customers will call one of the WCCs. Phone numbers can be found on the LDB Wholesale Operations website under "contact us" (<https://wholesale.bcldb.com/contact>).

2) The WCC call agent, who is an IAM administrator, will ask the customer for all 11 pieces of business information, filling out and submitting the online form for the customer

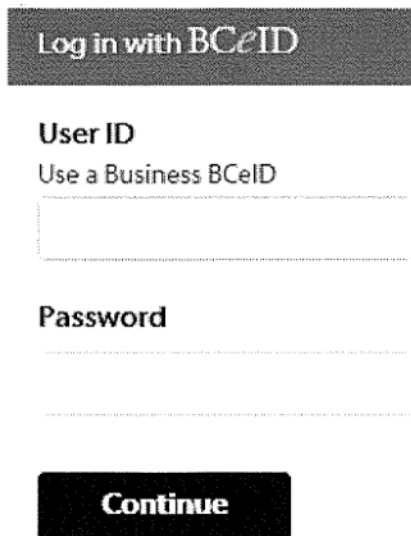
- License Number (i.e. valid license issued by Liquor Control Licensing Branch which authorizes you to purchase liquor from the LDB for the purpose of resale or a rural agency store or a duty free store authorized by the LDB)
- Company Name
- CRA Business Number
- Privacy BCeID
- First Name
- Last Name
- Address
- City
- Postal Code
- Phone
- Email

3) The WCC agent logs into their IAM administrator account and perform the following steps:

- a) Select "Create User from BCeID".
- b) Enter the BCEID supplied by the Wholesale Customer on the form. If there is a match the First Name, Last Name and Business Email address are displayed.
- c) They then click submit to add the account to the IAM system
- d) They then click "Manage Wholesale User"
- e) They search for the user entered in steps 2-5 by BCeID or Email address
- f) They enter the users contact information (address, phone number)
- g) They add one or more licence number as supplied by the Wholesale Customer.
- h) They click submit again.

4) The LDB IAM administrator from the LDB's Wholesale Customer team sends an email to the Wholesale Customer confirming that their IAM account has been created and that they can login to IAM and order online with their user name and password.

5) The Wholesale Customer logs in to Webstore using their BCeID account and password and order liquor product for the assigned Licence(s). The link to login to Webstore is available on the LDB's Wholesale website (<https://wholesale.bcldb.com/retailers>), as shown in the screen shot below.



Log in with BCeID

User ID
Use a Business BCeID

Password

Continue

Relationship between BCeID and IAM:

To clarify, the customer's BCeID user ID and password is used to authenticate their access to the LDB's IAM system. When the customer fills in their BCeID User ID and password, as per the above screenshot, a GUID (Globally Unique ID), which is a series of numbers and letters, is transferred from BCeID to IAM. This GUID in itself will not contain any personal information. It will consist of a series of numbers and letters but will not personally identify the individual. It will, however, be tied to that individual's BCeID and the BCeID site will have a record of the fact that the user made a request to be authenticated for the LDB's IAM Site. It will not know any further information about which application is being used nor what domain that application is using. This GUID will simply allow the IAM system to find the correct information for the user in IAM.

In addition, an API (Application Program Interface) is set up between IAM and BCeID system in order the following fields of business information to be transferred, along with the GUID from BCeID to IAM, only if there is an exact match with the BCeID user name that is supplied:

- First Name of Customer
- Last Name of Customer
- Business Email

Process for Creating a Sub-Account in IAM to Allow Other Individuals in their Business Access to the LDB's On-line Ordering System (WebStore).

The wholesale customer can request that a sub-accounts be created for other individuals in their business under their primary IAM account, i.e. if they have several restaurants and would like to give employees working at the different locations access to the system under separate accounts or if they would like to delegate the ability to order liquor to a an employee on their team. Here is a step-by-step process by which they can do this:

- 1) The wholesale customer who has already registered for WebStore (as described above) logs into their BCeID account and new (i.e. secondary) account to their primary BCeID account.

IX DMIP OR FOIPP COORDINATOR - REVIEW cont'd

During this process they submit the following information about the new secondary account holder:

- BCeID user name
- First Name
- Last Name
- Business Email Address

- 2) The Wholesale customer then log into their IAM account and selects "Create User from BCeID". They enter the BCEID user ID created in BCeID in Step 1

The IAM system then makes an API call to BCeID system and retrieves the GUID, First Name, Last Name and Email from BCeID if there is an exact match with the BCeID, as described above in the "Relationship between BCeID and IAM" section. If there is an exact match the First Name, Last Name and Business Email address are displayed.

- 3) They (primary Wholesale Customer) then clicks "Submit" button to add the account to the IAM account
- 4) They (primary Wholesale Customer) then click "Manage Wholesale User" "button".
- 5) They search for the user entered in steps 2-5 by BCeID or Email address. If there is a match the user's profile will appear.
- 6) They re-enter the users contact information (business address and business phone number) from the BCeID that was displayed in step 2.
- 7) They select one or more licences from the licence(s) they administer. The secondary user will be able to order liquor for the businesses who licenses they select.
- 8) They click the "Submit" button
- 9) They notify the secondary user that they have created a IAM account for them, sharing with them the secondary users BCeID userID and password they will need to login.

The secondary user can now log in to Webstore using their newly created BCeID user name and password and order liquor product for the assigned Licence(s).

5. Common or Integrated Program and Data-Linking Initiatives

		Yes	No
(a)	Does the original PIA (or the change now being considered) involve a "common or integrated program/activity", as defined in Schedule 1 of the <i>Freedom of Information and Protection of Privacy Act</i> (FOIPP Act)? * *Note: a "common or integrated program/activity" must be confirmed by regulation		X
(b)	Does the original PIA (or the change now being considered) involve a "data-linking initiative", as defined in Schedule 1 of the FOIPP Act?		X

IX DMIP OR FOIPP COORDINATOR - REVIEW cont'd

6. Purpose/Objectives of the revision (if statutory, provide citation).

Customer services for wholesale customers (i.e. in answer to their request to be able to delegate the responsibility of ordering product for their business.)

7. What are the potential impacts of this proposal?

As the new Wholesale Customer IAM Account initiative does not collect, use or disclose any further personal information from users than the original IAM PIA (for Special Occasion Licenses) and clear notification is given to Hospitality and Wholesale Customers regarding the collection and use of their personal information (i.e. the responses to their security questions) the LDB does not foresee this initiative having any privacy impacts.

Ministry Comments:

Privacy, Compliance and Training Branch Review and Comments

Simon Munn



February 6, 2018

Privacy Analyst
Privacy, Compliance & Training Branch
Corporate Information & Records
Management Office
Ministry of Citizens' Services

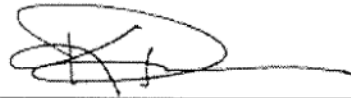
Signature

Date

X **SIGNATURES**

PUBLIC BODY APPROVAL:

Karine Bordua
Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General



Signature

February 7, 2018
Date

Scott Petersen
Enterprise Security Architect
Information Technology
Liquor Distribution Branch
Ministry of Attorney General



Signature

Feb 13, 2017
Date

Don Farley
Chief Information Officer Information
Technology
Liquor Distribution Branch
Ministry of Attorney General



Signature

Feb. 16, 2018
Date

Appendix A: Glossary of Useful Terms:

What is BCeID?

BCeID is an account that a member of the public, including an individual or a business can apply for in order to access online government services.

What is WebStore?

WebStore is an on-line ordering system used by LBD Wholesale customers to order product. Webstore is tightly integrated with LDB's Enterprise Resources Planning systems that support the Wholesale line of Business.

Who are Wholesale Customers?

Wholesale customers are "active" business customers who have a valid BCeID account, and have signed up for on-line ordering of liquor products from LDB Wholesale Customer Centre using WebStore. They are owners of Licensed Retail Stores (i.e. private liquor stores), large hospitality establishments (i.e. pubs and bars), Rural Agency (liquor) Stores, Independent Wine Stores and Duty Free customers.

What is the Wholesale Customer Centre?

The LDB has two Wholesale Customer Centres, one in Vancouver and one in Victoria. The Vancouver Wholesale Customer Centre services all Licensee Retail Stores, Rural Agency Stores, Independent Wine Stores and Duty Free stores operating in B.C. along with a selection of large hospitality customers. The Victoria location services hospitality customers in Greater Victoria



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

Part 1 – General

Name of Ministry:	Ministry of Attorney General, Liquor Distribution Branch		
PIA Drafter:	Manami Calvo, Information, Privacy & Access Services		
Email:	Manami.Calvo@bcldb.com	Phone:	604-252-3011
Program Manager:	Jeff Ring, Senior Manager , Wholesale Supply Chain, <i>Director</i> .		
Email:	jeffrey.ring@bcldb.com	Phone:	604-252-3819

1. Description of the Initiative

Under the oversight of the Ministry of the Attorney General, the BC Liquor Distribution Branch (LDB) is responsible for the purchasing, import, wholesale pricing, distribution and transportation of beverage alcohol in B.C. The *Liquor Distribution Act* gives the LDB the sole right to purchase beverage alcohol for resale within BC in accordance with the federal *Importation of Intoxicating Liquors Act*. As of December 5, 2018, LDB was tasked with providing non-medical cannabis wholesale and distribution services to the province. A new piece of legislation (i.e. *Cannabis Distribution Act*) outlines the LDB's role and responsibilities in wholesaling and distributing non-medical cannabis.

The non-medical cannabis wholesale and distribution mandate will translate into the following LDB wholesale and distribution cannabis business processes:

- The registration of non-medical cannabis products and accessories with the LDB for wholesale
- The receipt of non-medical cannabis products from licensed producers at the LDB's cannabis warehouse.
- The storage and management of these products in the LDB cannabis warehouse.
- The receipt of cannabis orders from publicly and privately-operated retail stores (i.e. B2B customers) as well as private customers (i.e. B2C customers) via the LDB's eCommerce system.
- The delivery of products to B2B retail stores and to the homes of B2C consumers.
- The return of cannabis product to LDB's cannabis warehouse due to fulfillment errors or failed delivery.



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

An interim process for registration of Licensed Producers (LPs) as LDB Vendors, and the registration of their non-medical cannabis products with the LDB for the wholesale supply chain will be needed in the timeframe of July 9th, 2018 – October 17, 2018 in order to stock the Distribution Centre for B2B and B2C customer needs, regardless of system readiness

Before describing this registration process, we have provided a glossary which will briefly describe three systems/applications referenced in this interim process:

- **E-Biz or Enterprise Resource Planning tool:** Enterprise resource planning is a category of business-management software that an organization can use to collect, store, manage and interpret data from many business activities. E-Biz is the short form of the enterprise resource planning software provided to us by Oracle E-Business Suite. This is a system that is housed on LDB servers in Canada.
- **E-Commerce System** – Portal by which LDB's wholesale and retail customers can order non-medical cannabis products delivered to their retail store or their homes.
- **GS1 Canada** – is a neutral, not-for-profit organization that develops and maintains global standards for efficient business communication across physical and digital channels. The LDB, along with a number of other Canadian provinces, will be asking all non-medical cannabis LPs who wish to sell their product wholesale through the LDB to register their product in GS1, making GS1 a central repository of core non-medical product attributes will allow for consistent industry standards and enable efficient sharing and maintenance of product information by licensed producers. Core attribute information includes barcodes, Global Trade Item Number (GTINs), pack sizes, product name, product categorization and other product attributes.
- **Item Master system or Cannabis Product Master (CPM)** - internal LDB database containing product information (e.g. size, type/classification) for LDB products. This is a system that is housed on LDB servers in Canada.

The interim registration process will be as follow:

1. LDB Vendor Relations Analyst will send a Vendor and Product Registration Letter via email to all LPs who have asked to register their product with the LDB. The letter will contain a generic username and password to the LDB Cannabis website, to allow LPs to access and download all forms needed for Vendor and Product Registration with LDB (i.e. Vendor Registration Form, Direct Deposit Application, BCLDB Product Attribute file.)



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes PIA#AG18044

2. LPs will complete the Registration Package, including registering their product in the GS1 central repository, and will be directed to send all information back to LDB electronically through email (cannabis.vendor@bclldb.com) or through other electronic means should their file be too large to send over email (i.e. through a file transfer system of their choice or through their website, etc.) .
3. LDB Vendor Relations Analyst will review the Registration Package for completeness of information.
4. LDB Vendor Relations Analyst will review GS1 file for quality assurance (QA) and will reach out to LP if there needs to be any changes to product attributes.
5. Once product submission will have passed QA, LDB Vendor Relations Analyst will enter product data into CPM application.
6. Product images and the BCLDB-specific attributes form will be sent to LDB Digital Merchandising Analyst for staging in the eCommerce system.
7. Vendor Registration Form and Direct Deposit Application will be sent to the LDB's Finance team who will set up the LP within eBiz, to set LPs up to be Vendors and enable LDB to pay for products that will be purchased.
8. LDB Vendor Relations Analyst will inform Wholesale Pricing that product is ready to be priced for wholesale.
9. LDB Pricing Analyst will price product for wholesale.
10. LDB Vendor Relations Analyst will inform LP that their product is now registered as an "active" product, via email.

The Cannabis project team expects this registration process to become more streamlined, for example the inputting of the LP's banking and product information to be less manual as integration is built between the vendor relations and wholesale websites. However the elements of data collected will remain the same. The planned long term process for LPs registration will be described in the LDB's Cannabis Wholesale PIA, currently in draft form.

2. Scope of this PIA

This PIA will assess the privacy implications of the interim process of Licensed Producers (LPs) registering as LDB Vendors, and the registration of their non-medical cannabis products and accessories with the LDB for the wholesale supply chain.



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

This PIA does not include:

- The interim process of issuing Purchase Orders for the LP's products
- The interim process of receiving product from the LP's and making payment to the LP's for their product.
- The interim process for the Customer Care Centre
- All of the long term processes after cannabis legalization on October 17, including the e-commerce system, wholesale processes, Customer Care Centre and Retail Returns.

3. Related Privacy Impact Assessments

AG18028 - Cannabis E-Commerce - Phase 1

4. Elements of Information or Data Collected from LP's for registration

The following business data elements will be collected from LP on the Non-Medical Cannabis Vendor Registration Application Package. **Please note that no personal information will be collected in this process:**

On Non-Medical Cannabis Vendor Registration Form:

- Contact Name
- Title
- Department (Accounts Payable, Sales or Others)
- Telephone
- Cellular Number
- Email address
- Company Legal Name
- Company Address
- CRA Excise License #
- CRA Excise License Start Date
- CRA Excise License End Date
- GST#
- Site Name
- Site Address
- Health Canada License #
- Health Canada License Start Date



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

- Health Canada License End Date
- Health Canada License Type
- Health Canada License Sub-Category
- Supporting documentation of licenses will be requested.

On Direct Deposit Application:

- Supplier Business Name:
- Vendor Number
- Address
- Telephone
- Cellular Number
- Email address
- Bank/Financial Institution Name
- Bank/Financial Institution Address
- Transit Number
- Institution Number
- Bank Account Number
- Financial Institution Verification (signature and bank stamp confirming accuracy of transit and account number)
- Signature of Authorized Supplier Representative
- Date Signed

On GS1 Product Registration File:

- Barcodes
- Global Trade Item Number (GTINs)
- Pack sizes
- Pack dimensions
- Product characteristics
- Product name
- Product categorization
- Other product attributes

On BCLDB Product Registration File:

- BCLDB-specific Short Description
- BCLDB-specific Long Description



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

- Inner/Master Pack Price
- Accolades
- Lineage
- Other attributes essential for BCLDB product publishing on the eCommerce system.
- Product Images of each product being registered



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Cole Lance

A handwritten signature in black ink, appearing to read "Cole Lance".

July 6, 2018

Privacy Analyst
Privacy, Compliance & Training Branch
Corporate Information & Records
Management Office
Ministry of Citizens' Services

Signature

Date



Privacy Impact Assessment for LDB Cannabis Interim Vendor and Product Registration Processes

PIA#AG18044

Part 7 – Program Area Comments and Signatures

Karine Bordua

Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 06, 2018

Date

Ian Bailey

Assistant Deputy Minister and Chief
Information Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 10, 2018

Date

Jeff Ring

~~Senior Manager~~ Director.
Wholesale Supply Chain
Liquor Distribution Branch
Ministry of Attorney General

Signature

July 11, 2018

Date

Michael Tan

Executive Director, Cannabis
Liquor Distribution Branch
Ministry of Attorney General

Signature

July 11, 2018

Date



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Part 1 – General

Name of Ministry:	Ministry of Attorney General, BC Liquor Distribution Branch		
PIA Drafter:	Manami Calvo, Information, Privacy and Access, Information, Privacy & Access Services		
Email:	Manami.Calvo@bcldb.com	Phone:	604-252-3011
Program Manager:	Renate Gross, Contractor - WMS Project Manager, Wholesale Services - Wholesale Supply Chain		
Email:	Renate.Gross@bcldb.com	Phone:	604 252-3703

1. Description of the Initiative

Under the oversight of the Ministry of the Attorney General, the BC Liquor Distribution Branch (LDB) is responsible for the purchasing, import, wholesale pricing, distribution and transportation of beverage alcohol in B.C. The *Liquor Distribution Act* gives LDB the sole right to purchase beverage alcohol for resale within BC in accordance with the federal *Importation of Intoxicating Liquors Act*. As LDB has the responsibility of the sole buyer and re-seller of wholesale liquor in the province's mixed public-private model, LDB is one of the largest liquor purchasers in the world. Every year, LDB buys alcohol from more than 1,000 Canadian and international suppliers and manufacturers, supplying product to wholesale and retail customers across the province.

To facilitate this, LDB has leased a 412,000 square foot warehouse in Delta, BC, which will become the principal distribution centre for LDB, scheduled to open in the summer of 2018. The LDB Delta Distribution Centre Project will provide a distribution centre with upgraded warehouse systems to increase operational efficiency, improve wholesale customer satisfaction and decrease operating costs. Within this project, the Warehouse Management System Work Stream (the "WMS Work Stream") will provide a new software backbone to the distribution function fulfilled by the LDB..

This stream has identified the WMS Liquor Solution (TECSYS), enabling technology that will make possible the improvements in efficiency, productivity and customer service that are a basis for the LDB distribution function. TECSYS will provide an integrated platform that will allow LDB to receive, put away, replenish, pick, assemble and ship products. It will draw in purchase and order information from the LDB legacy systems, and use that data to manage the warehouse activities. It will return confirmations of receipts and shipments, as well as inventory information to the LDB legacy systems. TECSYS will use the LDB's existing single-sign-on solution or it will provide an API (Application Program Interface) to obtain access to the single-sign-on capability.



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Implementing this solution will provide more flexibility for picking, labelling and shipping products to a high numbers of customers. To achieve this it will incorporate automated dimensioning/weighing capabilities and new RF (Radio Frequency) equipment. This solution will be used to manage the supply and distribution of liquor products from suppliers to the Distribution Centre and out to wholesale customers and retail stores.

2. Scope of this PIA

The scope of this PIA covers the new LDB Liquor Distribution Centre and LDB's use of TECSYS at its Liquor Distribution Centre. It includes:

- Collection of information, namely order/delivery management information
- Employee activity logs.
- Inbound advance ship notice from external suppliers directly and/or internal supplier portal including product description.

3. Related Privacy Impact Assessments

LDB 510 – Wholesale Order Management Web Store

SBRT 17004 - E-Biz Upgrade

SBRT 17004 – Wholesale Payments (EBS Upgrade)

SBRT 16015 – Identify Access Management (Initiative Update – Hospitality Product Catalogue)

AG 18005 – Identify Access Management (Initiative Update – Adding Secondary Users to LDB Hospitality Customers' IAM Accounts)

4. Elements of Information or Data

Before describing the elements of data, we have provided a glossary which will briefly describe the various systems/applications in the wholesale and distribution liquor business processes:

- **B2B Customers or Wholesale Customers** – B2B or Wholesale Customers are “active” business customers who have a valid BCeID account, and have signed up for on-line ordering of liquor products from LDB Wholesale Customer Centre using WebStore. They are owners of Licensed Retail Stores (i.e. private liquor stores), large hospitality establishments (i.e. pubs and bars), Rural Agency (liquor) Stores, Independent Wine Stores and/or Duty Free customers.



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

- **Data Warehouse:** the Data Warehouse is a corporate computer system used at the Branch to collect and store business and personal information so that it may be retrieved to answer queries, produce reports, and explore and analyse data. The objective of the Data Warehouse is to provide storage for relevant business information so that individuals with approved access will be able to quickly and easily retrieve information on a timely basis to support and make better business decisions. The information stored will be used for analysis and NOT for permanent archiving
- **E-Biz or Enterprise Resource Planning tool:** Enterprise resource planning is a category of business-management software that an organization can use to collect, store, manage and interpret data from many business activities. E-Biz is the short form of the enterprise resource planning software provided to us by Oracle E-Business Suite. This is a system that is house on LDB servers in Canada.
- **Enterprise Store Operations (ESO):** an application providing operational, cash, supply chain, inventory, merchandise, and financial management to the LDB head office and its stores. ESO draws sales information from POS (Point of Sale System – see below glossary term) and provides the LDB head office with sales-related reports from stores. This is a system that is house on LDB servers in Canada.
- **Point of Sale (POS) system:** system which collects information from a customer in order to make a payment to the merchant in exchange for goods (i.e. credit card information)
- **Item Master system** - internal LDB database containing product information (e.g. size, type/classification) for LDB products. This is a system that is housed on LDB servers in Canada.
- **Wholesale Costing & Pricing system (WCP):** an application used to calculate the wholesale price. WCP uses the CAPS database. This is a system that is house on LDB servers in Canada.

Data Elements in WMS:

1. Business Information:

- B2B Business customer name
- Names of primary/authorized contacts
- Shipping address
- Business phone number
- Product information (e.g. size, type/classification)
- Inventory adjustments/ Inventory records/ Cycle count data
- Special order returns (including recalls) – product information and quantity but does not include customer name or address



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

2) Personal Information:

- **Employee master data:**
 - Name
 - Login ID
 - Employee number
 - Job title
- **Employee task performance data:**
 - Sign-in to system time
 - Sign-out of system time
 - Audit trail of interactions with inventory such as time logs of task performed (i.e. scanning in product, scanning out product, checking inventory, etc.). Includes goal time generation (i.e. a task is assigned to an employee and it would be expected to be completed in a reasonable amount of time)
 - Performance metrics (i.e. time taken to complete task once assigned)

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information of the WMS solution will be stored on LDB servers in Canada and will be accessible within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Employee logs on to WMS system, resulting of a time stamp of when they began working. Collected data includes their user ID and the time they logged in.	Collection	26(c) and (e)
2.	Employee interacts with a product/uses a piece of machinery resulting in a log of their activity while working. Log includes the user ID, the time the activity was performed, and what activity was performed. For example, an employee may be assigned to ship 20 items to a liquor store. The employee would receive the order information and what machinery is required to complete the order. The employee would go to the location and "pick" the 20 items which would be logged as an activity. The Stagers will take the picked items to the shipping lane which will be logged as well.	Collection	26(c) and (e)



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

3.	Manager access information to manage task performance. A manager may wish to see whether a task was completed, how long it took for an employee to complete the task, and what actions they performed along the way. The manager may notice discrepancies with the task such as an unusual amount of time for a task to be completed, or an employee reporting fewer items available for "picking" than the WMS believes to be in-stock. The manager may use this information to manage the employees' performance or recommend an investigation to Corporate Loss and Prevention or Labour Relations.	Use	32(a)
4.	Corporate Loss and Prevention and/or Labour Relations investigate employee behavior to determine if a violation of the Code of Conduct and/or a crime has been committed.	Disclosure and Use	33.2(a), and 32(a)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes	Oath of Employment Standards of Conduct Privacy training for LDB employees and contractors Criminal Records Check	Low	High
2.	Data may be compromised by an attack on LDB servers from an external threat.	Technical security measures	Medium	Low
3.	Employees may use each other's ID cards or login credentials, resulting in the collection of incorrect information	BC LDB's Conditions for Use of Information Technology	Medium	Low



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

10. Collection Notice

When employees are given access to the WMS, they will be given the following notification:

"Please note that when you login to the WMS your activity will be logged for performance management, training and program improvement purposes pursuant to section 26(c) and (e) of the *Freedom of Information and Protection of Privacy Act*. If you have any questions please ask your supervisor. If you have further questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5."

Part 3 – Security of Personal Information

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

LDB servers are kept in a locked building. Access to the building is only possible to employees with a key card, or to guests who have signed in at reception and are accompanied by an employee. Physical security measures for the warehouse building are as follows:

- High security locks and keys
- Perimeter gate controls
- Key card required for access. Each key card is associated with a specific employee and access swipes are logged and auditable
- 24/7 surveillance in warehouse building and on exterior of building
- 24/7 security personnel on-site
- Locked cabinets for shipping lists and un-affixed labels
- After-hours alarm system which notifies security and police in the event the alarm is triggered

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

LDB Servers are secured through the following security measures:

- Robust network security architecture including firewalls
- Encryption of all data in transit
- Individual accounts for all access to data. (i.e. no generic accounts)
- Full Audit Log of system activities
- A STRA will be done on WMS by LDB's internal security team before it is launched

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

The LDB has its own Information Security Policy. It is based on the government's Information Security Policy. In turn both of the policies are based on ISO 27001 security standard.



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Consequently LDB policy is consistent with Government's but has been adapted for the LDB Environment.

- 14. 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.**

Data is restricted to role-based access.

- 15. Please describe how you track who has access to the personal information.**

Access to personal information within the system will be logged and the logs will be auditable.

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. 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?**

Information cannot be updated because it consists of activity that is automatically logged. Information may be incorrectly associated with an employee. Employees will have the ability to notify their supervisor in such an instance. If an employee disputed the accuracy of the log, a note would be made to the file.

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

Yes. Data will be used to manage employee task completion and performance as per the activity logs.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

The employee identification is verified upon hire and when provided the relevant ID access card. LDB policy states that LDB employees must use their own login credentials to access services and their own IDs to access restricted areas.

- 19. If you answered "yes" to question 17, 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?**

Yes, IT logs are kept for 2 years prior to disposition.



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Part 5 – Further Information

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

No.

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

No.

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

Yes.

Personal Information Bank – Required Information	
Description	Wholesale Management System Liquor
Primary ministry/government agency involved	Ministry of the Attorney General/ Liquor Distribution Branch
All other ministries/government agencies and public bodies involved	N/A
Business contact title	Director – Warehouse Operations
Business contact telephone number	604 252-3129



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Mike Corcoran

Privacy Analyst
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

July 17, 2018

Date

Dwayne McCowan

A/Sr. Privacy and Policy Advisor
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

July 19, 2018

Date



Privacy Impact Assessment for Warehouse Management System Liquor

PIA# AG18046

Part 7 – Program Area Comments and Signatures

Karine Bordua
Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 22, 2018

Date

Ian Bailey
Assistant Deputy Minister and Chief
Information Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 25, 2018

Date

Ken McDonnell
Director- Warehouse Operations
Liquor Distribution Branch
Ministry of Attorney General

Signature

Date

R. Blain Lawson
General Manager
Liquor Distribution Branch
Ministry of Attorney General

Signature

08/8/2018

Date



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes

PIA#AG18064

Part 1 – General

Name of Ministry:	Ministry of the Attorney General, Liquor Distribution Branch		
PIA Drafter:	Manami Calvo, Information, Privacy & Access Services		
Email:	Manami.Calvo@bcldb.com	Phone:	604 252-3011
Program Manager:	Cisco Pacheco, Manager, Customer Care Centre, Cannabis Operations		
Email:	Cisco.Pacheco@bcldb.com	Phone:	604-252-3007

1. Description of the Initiative:

Under the oversight of the Ministry of the Attorney General, BC Liquor Distribution Branch (LDB) is responsible for the purchasing, import, wholesale pricing, distribution and transportation of beverage alcohol in B.C. The *Liquor Distribution Act* gives LDB the sole right to purchase beverage alcohol for resale within BC in accordance with the federal *Importation of Intoxicating Liquors Act*. As of December 5, 2017, LDB has also been tasked with providing non-medicinal cannabis wholesale and distribution services to the province of BC. Effective February 5, 2018, LDB has also been given responsibility for retailing non-medicinal cannabis online and alongside private retail stores. The *Cannabis Distribution Act* has recently been enacted which outlines LDB's role and responsibilities in distributing and retailing non-medical cannabis.

To meet this new mandate, LDB is launching an e-commerce platform that will allow its wholesale and retail customers to purchase non-medical cannabis online as well as opening BC Government operated retail cannabis outlets (BC Cannabis Stores or BCCS) that will allow its retail customers to purchase non-medical cannabis and cannabis products in government stores.

To track and manage customer interactions and improve customer satisfaction, LDB is launching a Customer Care Centre (CCC) to service its non-medicinal cannabis wholesale and retail customers. "Wholesale" customers are privately owned or government owned non-medical cannabis stores who will order non-medical cannabis for resale at their own retail stores. "Retail" customers are individual consumers who will purchase non-medical cannabis either through LDB's e-commerce platform or LDB's BC Cannabis stores.

Although anyone will have the ability to call the CCC with inquiries related to cannabis products and/or cannabis accessories, the primary purpose of the CCC will be to service retail and wholesale customers who have ordered cannabis products/accessories from the LDB's e-



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes

PIA#AG18064

commerce platform. The CCC will be staffed by LDB employees and will utilize a Customer Relationship Management (CRM) tool to track and manage customer inquiries and issues.

An interim CRM tool will be needed for the CCC in the first phase of the LDB cannabis business until a fully functional CRM tool can be procured and implemented. This interim CRM tool will be SharePoint CRM software, which will be housed on LDB servers located in Canada and which will be used to track and record all CCC interactions with customers that come in via phone calls, emails and webforms. CCC agents will be using forms to accomplish the following CRM related tasks:

- Assign a ticket numbers to every customer inquiry;
- Centrally document all interactions between customers and CCC agents;
- Have a single view of all contact and business information of customers who contact the CCC via telephone, voicemail, email or webform;
- Track and record completed Product Return Merchandise Authorization (RMA) forms for returned products and link it to the customer CCC ticket number;
Track and record order cancellations that are called in by customers;
- Provide a single repository of knowledge items by having a Knowledge Database of all cannabis products and accessories accessible to CCC agents;
- Provide standard reports based on customer data elements collected on the forms.

For the interim process there is no integration between the interim CRM tool and any other LDB systems. Separate access to other LDB systems will be required by CCC agents to answer customer inquiries and in order to access customer order history and order status and provide product information. These systems will be the e-commerce system, the Identify Access Management (IAM) system, the Oracle eBiz system, the Warehouse Management System, the Enterprise Store Operation, the Marval's Integrated IT Service Management, the Cannabis Product Master, the Knowledge Database, the Telus Call Centre (TC3), and the Data Warehouse. Note that PIAs are or have been completed for the e-commerce and the IAM system, the TC3, the Warehouse Management System and Marval's Integrated IT Service Management.

The E-Commerce and the IAM system:

The e-commerce system is the platform by which wholesale and retail customers order cannabis online. IAM is the access system used to control and verify all user system access. The privacy implications of these systems are covered in PIA AG18028.



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes

PIA#AG18064

- CCC agents will need to access information in the e-commerce system to verify customer identity when the customer calls in (i.e. to ensure they are speaking to the customer who owns the account).
 - CCC agents will need to access information in IAM to:
 - Verify customer contact information (i.e. customer name, email address);
 - Verify customer current order information (i.e. what product the customer has on order with BCCS online);
 - Verify customer purchase history (i.e. what products they have ordered from e-commerce in the past and when);
 - Access the customer's order status to update customer; and
 - Cancel orders and give refunds to customers.
 - CCC agents will also need to access information in IAM to:
 - Reset customers' IAM account passwords.
- **Oracle eBiz and Enterprise Store Operations (ESO)**
 - Oracle eBiz is the primary financial system and it will house non-medical cannabis customer return information.
 - CCC agents will need to access to the information in Oracle e-Biz to do financial adjustments to customer accounts when processing returned product.
 - ESO is an application providing operational, cash, supply chain, inventory, merchandise, and financial management to the LDB head office and its stores. ESO draws sales information from the Point of Sale system (i.e. the credit/debit card pinpads) and provides the LDB head office with sales-related reports from BC Cannabis Stores.
 - CCC agents will need to access information in ESO to answer requests for inventory and product information from customers.
 - **Warehouse Management System**
 - WMS track and control all incoming and outgoing inventory.
 - CCC agents will need to access to information in WMS to:
 - Cancel orders to restore stock, verify product inventory and process RMAs
 - Find the status of a customer's order (i.e. if it has left the LDB warehouse, is on route to their shipping address, etc.)
 - Create shipping labels for customers so that the customers can print out and ship back returned products to CCC.



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

- **Marval's Integrated IT Service Management (MSM)**
 - The process of logging a ticket for customers who call into the LDB's Support Centre is described in SBRT 17008 – LDB Marval's Integrated IT Service Management.
 - CCC agents will need to access to information in MSM to:
 - Open a ticket in MSM which has been escalated to them from the LDB's Support Centre team in order to find out the nature of the inquiry and to access the contact details of the customer in order to call or email them back.
- **KBdB (Wiki)**
 - The KBdB will be a general reference source for CCC agents. It will contain information on cannabis products (or a link to where to find specific info) as well as FAQs and Standard Operating Procedures, for example where to find what information in the various LDB systems to answer customer inquiries, etc.
 - No personal information will be contained in KBdB.
 - CCC agents will need to access to information in KBdBWik to:
 - To verify how to do various work tasks and find general information on cannabis products to respond to caller inquiries
- **Cannabis Product Master(CPM)**
 - The master file containing information on attributes of all cannabis products and accessories.
 - No personal information will be contained in CPM.
 - CCC agents will need to access to information in CPM to:
 - Look up detailed attributes of the cannabis products and accessories that LDB carries in order to answer customer inquiries.
- **TC3 (Call Centre Anywhere)**
 - TC3's Work Force Management application Verint will be used to manage and monitor CCC staff performance. The system and the relevant process have been assessed as part of SBRT 17001 (Call Centre Anywhere Upgrade) and the 2018 PIA Update.
 - CCC supervisors will need to access to information in TC3 to:
 - Manage employee schedules, perform QA to ensure consistent caller experience, add/delete CCC team members in the system once they leave the company.



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

- **Data Warehouse**

- The Data Warehouse is a corporate computer system used at LDB to collect and store business so that it may be retrieved to answer queries, produce reports, and explore and analyse data. The objective of the Data Warehouse is to provide storage for relevant business information so that individuals with approved access will be able to quickly and easily retrieve information on a timely basis to support and make better business decisions. The information stored will be used for analysis and NOT for permanent archiving.
- Individual customer sales information will not be housed in the Data Warehouse. The process of liquor customer return information flowing into the Data warehouse is described in PIA SBRT 16006 – LDB Customer Returns.
- The application is housed on LDB servers located in Canada.
- CCC access to Datawarehouse is required to:
 - Produce ad hoc reports on number of customer returns (i.e. customer returns per store, per Branch). These reports will be produced at an aggregate level and will not contain customer personal information.

2. Scope of this PIA

This PIA will assess the privacy implications of the CCC's processes. The following are out of scope of the PIA:

- Collection, use and disclosure of voice recordings and performance metrics of LDB's telephony system, which is covered in the LDB's Call Centre Anywhere PIAs listed in section three below:
- The BCCS return process, including retail customer interaction and the collection of customer information.

3. Related Privacy Impact Assessments

SBRT17001 – Call Centre Anywhere (TC3)

SBRT17001 – Call Centre Anywhere – Initiative Update (TC3)

AG18045 – LDB Call Centre Anywhere PIA Update

AG18028 – E-Commerce Platform



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

SBRT 17008 – LDB Marval's Integrated IT Service Management

JAG15038 - Identity Access Management

AG18005 - Webstore Update

SBRT16005 – LDB Retail Sales Tracking and Reporting

AG18030 – LDB Cannabis Wholesale and Distribution

AG18040 – LDB Cannabis Customer Retail Returns

4. Elements of Information or Data

The following elements of information may be collected directly from customers when they contact the CCC to verify their identity and to answer questions regarding their account and process their inquiry:

- First and last name
- Home or business address
- Personal or business email
- Order details and status
- Description of inquiry
- Purchase date and history
- CCC Inquiry history
- Order/tracking number
- Responses to IAM security questions and responses (i.e. what is your mother's maiden name) – if customer request to have their password reset.
- Age verification (confirmation that they are over 19 years of age)
- Personal or business phone number
- Shipping info
- Description of Return
- Purchase quantity
- Return quantity
- Business license



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes

PIA#AG18064

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All the personal information stored on interim CRM tool will be housed on the LDB servers located in Canada and will only be accessed from Canada.

The storage and access of the information on the e-commerce system, the IAM system, the ESO, the WMS, the MSM have been previously assessed in different PIAs.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. The datalinking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/A

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Personal Information Flow Table – Customer Requests/Inquiries			
	Description/Purpose	Type	FOIPPA Authority
1.	Customer calls, emails, or contacts the Cannabis Customer Care Centre through the e-commerce webform to request information. Customer provides personal information to confirm age, verify identify and address the caller's inquiry. Age verification includes a positive indication of legal age in the medium used (e.g. telephone, email exchange). CCC staff will not request that customers scan their ID, a verbal or written statement of legal age will be acceptable. Age verification information is not retained, but is used to make a determination about the ability to proceed with the customer through the customer interaction.	Collection	26(c)
2.	MSM tickets are received by CCC staff from Support Centre, reviewed, and verify to confirm that it is a customer support issue.	Collection Use	26(c) 32(a)
3.	CCC agent contacts customer back to gather more information/clarification if necessary.	Use Disclosure Collection	32(a) 33.1(7) 33.2(a) 26(c)
4.	CCC staff accesses different LDB systems and utilizes necessary information to resolve issue.	Use Collection	32(a) 26(c)

For PCT Use Only:
Version 1.0



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

		Disclosure	27(1)(b) 33.2(a) and (c)
5.	CCC staff provides information back to the customer to answer the caller's inquiry.	Disclosure	33.2(a)
6.	Inquiry is resolved. SharePoint form is updated and ticket is closed.	Use	32(a)

Personal Information Flow Table – Product Return

	Description/Purpose	Type	FOIPPA Authority
1.	CCC agent receives information from an RMA form and verifies the information.	Collection Use	26(c) 27(1)(b) 32(a)
2.	CCC agent logs into Canada Post and creates a shipping label	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a)
3.	CCC agent emails the shipping label to the customer	Disclosure Use	33.1(7) 33.2(c) 32(a)
4.	Customer prints out shipping label and present label to Canada Post staff to return the package to LDB.	Collection Use	26(c) 32(a)
5.	CCC agents verify returned item against the RMA information.	Collection Use	26(c) 32(a)
6.	If RMA is approved, CCC issues customer refund via e-commerce system and customer is sent notification via email through the e-commerce system that the RMA has been approved and a refund has been issued to them. If RMA is not approved, customer is sent notification via email through the e-commerce system that the RMA has been rejected & reason for rejection.	Use Disclosure	32(a) 33.2(a)



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

7.	Inquiry is resolved. SharePoint form is updated and ticket is closed.	Use	32(a)
----	---	-----	-------

Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes.	Privacy Training; Oath of Employment; Code of Conduct; Access to personal information limited to a select number of LDB employees; Access will be logged; and Audit trails.	Low	Low
2.	Outside authorized system access to view personal information.	Authentication through Active Directory, Defined SharePoint access, Defined User Roles for each system application, Secured Building	Low	High

9. Collection Notice

Retail customers who call the CCC will be given the following message:

"Please note this call we will be recorded for training and program improvement purposes. Any personal information that you provide during this call will be collected by the Liquor Distribution Branch under 26 (c) and (e) of the Freedom of Information and Protection of Privacy Act, in order to respond to your request for assistance. If you have any concerns please ask the next available representative. If you have further questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5."

The following notice will be placed on the CCC webform:

"Your personal information is collected on this form in order to answer your inquiry, provide you information on your order and/or process your return. This information is collected pursuant to s.26(c) and (e) of the Freedom of Information Protection of Privacy Act. If you



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

have any questions, please contact the LDB's Privacy Officer at 604-252-3043 or write them at 2625 Rupert Street, Vancouver, B.C., V5M 3T5."

Part 3 – Security of Personal Information

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

The personal information stored on the interim CCC CRM tool will be housed on LDB servers located in Canada.

LDB servers are kept in a locked building. Access to the building is only possible to employees with a key card, or to guests who have signed in at reception and are accompanied by an employee. Physical security measures for the warehouse building are as follows:

- High security locks and keys
- Perimeter gate controls
- Key card required for access. Each key card is associated with a specific employee and access swipes are logged and auditable
- 24/7 surveillance in warehouse building and on exterior of building
- 24/7 security personnel on-site
- Locked cabinets for shipping lists and un-affixed labels
- After-hours alarm system which notifies security and police in the event the alarm is triggered

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

LDB Servers:

- Robust network security architecture including firewalls
- Encryption of all data in transit
- Individual accounts for all access to data. (i.e. no generic accounts)
- Full Audit Log of system activities.

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

The LDB has its own Information Security Policy. It is based on the government's Information Security Policy. In turn both of the policies are based on ISO 27001 security standard.

Consequently LDB policy is consistent with government's Information Security Policy but has been adapted for the LDB Environment.



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

13. 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.

All internal LDB users with valid Active Directory credentials will have the ability to authenticate to SharePoint.

Authorization will be managed through Active Directory groups. This approach will leverage existing or new Active Director Groups as a means of defining the membership of SharePoint roles. The SharePoint roles will be assigned permission to SharePoint sites, folders or documents.

Only a limited number of roles will be assigned as administrator role that will have the ability to delete or modify documents. CCC Management will review and approve the access policy to the CCC SharePoint site. The access model will be reviewed regularly by CCC Manager and IT Security staff.

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

Access to personal information within the system will be logged in SharePoint and the logs will be auditable.

Part 4 – Accuracy/Correction/Retention of Personal Information

15. 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?

Customers will have the ability to contact the CCC at any time to correct, update, annotate or verify personal information about them. If the personal information is provided to another party in the past 12 months, they will be notified of the request.

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

Yes, the initiative will use personal information to change or cancel their online orders.



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

- 17. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

Action such as changing or cancelling a customer order will only be done if customer is able to correctly answer the verifying questions, to ensure they are the owners of their E-Commerce account.

- 18. If you answered "yes" to question 17, 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?**

Yes. LDB has an approved records retention and disposition schedule to ensure that any information is kept for at least one year after it is used in making a decision directly affecting an individual.

Part 5 – Further Information

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

No.

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

No.

- 21. Will a personal information bank (PIB) result from this initiative?**

Yes.

Personal Information Bank – Required Information	
Description	Liquor Distribution Branch's non-medicinal cannabis wholesale and retail customer interactions.
Primary ministry/government agency involved	Ministry of Attorney General, Liquor Distribution Branch
All other ministries/government agencies	N/A



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

and public bodies involved	
Business contact title	Customer Care Centre Manager
Business contact telephone number	604 252-3007



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes PIA#AG18064

Part 6-PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry

Privacy Advisor
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

October 15, 2018

Date

Rhianna Begley

A/Director, Strategic Privacy
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

October 15, 2018

Date



Privacy Impact Assessment for Cannabis LDB Customer Care Centre Processes

PIA#AG18064

Part 7-Program Area Comments and Signatures

Karine Bordua

Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General

Signature

October 16, 2018

Date

Ian Bailey

Assistant Deputy Minister and Chief
Information Officer
Information Systems Branch
Ministry of Attorney General

Signature

October 16, 2018

Date

Michael Tan

Executive Director Cannabis
Liquor Distribution Branch
Ministry of Attorney General

Signature

10/18/18

Date

Blain Lawson

CEO and General Manager
Liquor Distribution Branch
Ministry of Attorney General

Signature

10/24/18

Date



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Part 1 – General

Name of Ministry:	Ministry of the Attorney General, Liquor Distribution Branch		
PIA Drafter:	Manager, Information, Privacy and Access Services		
Email:	Manami.Calvo@bcldb.com	Manami.Calvo@bcldb.com	Phone: 604-252-3000
Program Manager:	Michael Tan, Executive Director, Cannabis		
Email:	Michael.Tan@bcldb.com		Phone: 604-252-3872

1. Description of the Initiative

Under the oversight of the Ministry of the Attorney General, the BC Liquor Distribution Branch (LDB) is responsible for the purchasing, import, wholesale pricing, distribution and transportation of beverage alcohol in B.C. The *Liquor Distribution Act* gives the LDB the sole right to purchase beverage alcohol for resale within BC in accordance with the federal *Importation of Intoxicating Liquors Act*. As of December 5, 2017, LDB has been tasked with providing non-medical cannabis wholesale and distribution services to the province. In addition, on February 5, 2018, LDB was also given responsibility for retailing non-medical cannabis, alongside private cannabis retail stores. The *Cannabis Distribution Act* outlines the LDB's role and responsibilities in distributing and retailing non-medical cannabis.

To meet this new mandate, the LDB is opening BC Cannabis Stores (BCCS) and launching an e-commerce platform that will allow its wholesale and retail customers to purchase non-medical cannabis. Note that "wholesale customers" are defined as privately owned or government owned non-medical cannabis stores and "retail customers" are defined as individual consumers. As the LDB's e-commerce platform will be the tool by which LDB distributes non-medical cannabis to both its wholesale and retail customers, it will be the foundation of the LDB's non-medical cannabis program and all other operational streams of the LDB's e-commerce program (Retail, Wholesale, and Customer Care Centre streams) will be reliant on the functioning of this stream. The wholesale processes have been assessed as part of a previous PIA.

The retail website will be the portal by which retail customers order cannabis products for their personal consumption. Personal information will be collected through this website in order to:

- Enable distribution of online orders for fulfillment and inventory management through integration into the LDB's Warehouse Management System (WMS);
- Integrate the e-commerce solution to support all required LDB systems; and



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

- Provide ongoing support to LDB Customer Care Staff and IT Support staff with a dedicated account management team, specific training resources for online technology and 24/7, live global support.

For more detail descriptions of the systems see Appendix A.

Services, software, and hardware on LDB's e-commerce system and the above related systems will enable LDB non-medical cannabis customers to create an e-commerce account, select products, pay for the products, submit an order, and have the order delivered to their home address (retail customers).

For the creation of the e-commerce solution, LDB has selected Shopify Inc., a Canadian company. The solution will enable e-commerce management, web content management, experience management (i.e. how users will experience our website based on our homepage content, website taxonomy, website usability), order management, transaction management, product management, and reporting. To clarify, data extraction and reporting for the project will include reporting based on sales/transaction information collected in our e-commerce system as customers order product in the system (i.e. most popular items sold, how much of what product was sold in a day and high level stats such as aggregate number of visits to the website, etc.). Aggregate reporting will not contain personal information.

Shopify will work in partnership with the following sub-contractors to provide the services described below under Shopify's contract with the LDB:

- 1) Google Cloud Canada – The solution is a Software-as-a-Service and it will be hosted and maintained by Shopify on Google Cloud Canada servers.
- 2) Pixel Union – Pixel Union, a Canadian company, will be building the websites that will allow Shopify to provide webstore services to its retail and wholesale customers. Pixel Union will also integrate the e-commerce tool into LDB systems (Identity Access Management (IAM), WMS and Customer Care Centre). They will also be providing LDB with technical support.
- 3) TaskUs – To enable 'follow the sun' service and 'around the clock' system support, TaskUs will provide LDB Customer Care Centre staff and IT Support Centre staff with overnight technical support in the off-hours when Shopify and Pixel Union's technical teams are not available to provide LDB technical support.

Orders submitted via the LDB's e-commerce system will be processed by the LDB non-medical cannabis warehouse team, packaged and submitted to Canada Post for retail customer deliveries who will deliver the order to the customer's provided address.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Age verification will be done on all retail customers upon delivery, either visually (i.e., verifying if they look over 25) or, if the customer looks to be under 25 years of age, through photo ID verification. Canada Post staff will record whether age verification was done visually or through photo ID for each customer. No copy of the ID will be retained on behalf of the LDB.

Additional LDB PIAs have been drafted to cover other areas of the non-medical cannabis program, all of which will have components that are related to the e-commerce initiative. These PIAs will cover:

- LDB Customer Care Centre
- Wholesale/Supply Chain
- Customer Returns at BC Cannabis Stores

Additional PIAs will also cover the licensing and enforcement of Cannabis and will be conducted by the Liquor Control and Licensing Branch of the Ministry of Public Safety and Solicitor General.

2. Scope of this PIA

This PIA will assess the privacy implications of the e-commerce initiative of the non-medical cannabis mandate of the LDB, including the online ordering and delivery for retail consumers and the distribution of non-medical cannabis products to retail customers who order cannabis on the LDB's e-commerce system and have it delivered to their home.

The PIA will also describe the return process in a "Return to Sender" scenario, when product is returned to the LDB warehouse without having been delivered to the customer.

3. Related Privacy Impact Assessments

FIN15017 – Express Pay 2.0 Lite hosted by Beanstream (Beanstream has been renamed Bambora, and will be referred to as Bambora throughout this PIA)

JAG15038 – Identity Access Management

SBRT16005 – Retail Sales Tracking and Reporting

AG18040 – LDB Cannabis Customer Retail Returns

AG18046 – Warehouse Management System Liquor



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

AG18058 – LDB Cannabis Wholesale and Distribution

AG18064 – Cannabis Customer Care Centre

4. Elements of Information or Data

Reporting

- Reporting based on sales/transaction information collected in LDB's e-commerce system as customers order product in the system (i.e. most popular items sold, how much of what product was sold in a day and high level stats such as aggregate number of visits to the website, etc.)
- No personal information will be included in the reporting

Retail Customers:

Retail customers will have the option of creating an LDB account (using LDB's IAM) before submitting an order on the e-commerce platform or simply proceeding directly on the e-commerce platform and submitting their order as a guest.

The advantage to creating an LDB account on IAM is that certain information collected in the customer's IAM account (i.e. name, email, address) will be pulled from the customer's IAM account and pre-populate the customer's order form in the e-commerce system. In addition, customers with an account can login to their account and view their order history (up to eight years).

Retail customers provide the following information when they fill out the registration page for setting up an account in IAM:

- Age verification – customer is asked to tick a box to confirm they are over the age of 19. This data is not saved – rather the customer is able to proceed with the creation of an account and will not be allowed to proceed to create an account if they do not click on the tickbox.
- First Name
- Middle Initial(s) (optional)
- Last Name
- Email Address
- Primary Phone Number
- Alternate Phone Number (optional)
- Shipping Address (multiple)



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

- Address Block
 - City
 - Postal Code
- Answers to three self-selected security questions (i.e., what was the name of your first pet?)
- Username
- Password
- Audit records: activities of user, activities of system administrators, denied authorisations, denied resources, admin operations by administrator.

When a customer has an IAM account, the following information will be pulled from IAM into the e-commerce platform when the customer clicks on the “order” icon:

- Customer’s first and last name
- Email address
- Shipping address

Customer will then enter the following additional information:

- Order details
- Credit card number
- Card security code (CVV)
- Expiry date of credit card
- Cardholder Name
- Billing address
- Shipping preferences (e.g. method or tier such as express delivery).

If a retail customer does not have an IAM account, the following information will be required from the customer when placing an order:

- Age verification of retail customer

Customer will be asked to input their Date of Birth (DOB) into the e-commerce system. The system will automatically calculate whether the DOB supplied by customer meets the criteria of the customer being over 19 (i.e. if today’s date is April 15, 2018 than any date before April 14, 1999 will be rejected and any date after April 15, 1999 will be accepted).



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Please note that the actual DOB digits will NOT be stored on the e-commerce system, rather the fact that the customer age verification digits were accepted by the system, meaning they have said they were over the age of 19 is stored. It should be noted for clarity, that legal age for consumption will be confirmed by the delivery service at the time of delivery.

- Client First Name
- Client Last Name
- Client Billing Address
- Email address
- Order details (shipment/order contents, weight, order time, delivery time, etc.)
- Shipping Address (must be in province of British Columbia)
- Credit card number
- Card security code (CVV)
- Expiry date of credit card
- Cardholder Name
- Billing address
- Shipping preferences (e.g. method or tier such as express delivery).

Note that the credit related data elements will be entered in LDB's e-commerce platform but will be instantaneously transmitted immediately to TD Bank through Bambora/BC Pay Express). Through integration with e-commerce and Bambora/BC Pay Express these data elements will never be stored on the e-commerce platform but rather will flow straight through to Bambora/BC Pay Express.

The email addresses of retail customers will be used to send follow up emails on their order and other such communication as is necessary in the ordinary course of their relationship with LDB.

Those emails will be for the following purposes:

- Account activation confirmation
- Account edit instructions(optional – only if necessary)
- Forget password flow (optional – only if necessary)
- Order creation confirmation
- Order ship update(full shipment, partial shipment, short shipments)
- Order refund/return confirmation
- Order cancellation confirmation(optional – only if necessary)
- Recall notification



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

- Return authorization email (optional – only if necessary)
- Return confirmation email
- Shipment tracking information
- Order shipping update
- Availability of stock (i.e., if stock is out, customer may opt to be notified when product is restocked)
- Future opportunities to sign up to receive promotional materials.

The following personal information of retail customers will be transmitted from the LDB e-commerce system to WMS:

- First name
- Last name
- Shipping address
- Phone number
- Email address
- Order line details (SKU#, SKU description, quantity ordered, etc.)
- Reason for returns, if customer is returning product

The following data elements of retail customers will be transmitted from LDB to Canada Post through Secure File Transfer Protocol (SFTP):

- Shipping address
- Weight of package
- Service Type (i.e. Express Delivery, etc.)
- Tracking number

The following personal information of retail customers will be transmitted from Canada Post to LDB via SFTP:

- Order status updates of package (e.g. "Package picked up from depot", "Order successfully delivered", "Package picked up at PO", "Return to Sender")
- For packages returned to sender, generic reason for the RTS status (i.e. incomplete address, refusal of delivery)



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

The following personal information of retail customers will be collected directly by Canada Post at the time of package delivery:

- Age verification (i.e. whether age verification was done visually or through photo ID)
- Signature of customer

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Storage of Data

The Google Canada's cloud data center, where LDB e-commerce customer information will be stored, is located in Google Canada's Montreal facilities, including back-ups.

Transmission of Data

There will be two sovereign route connections that will carry LDB data from Google Canada's cloud data center to LDB servers:

- 1) Connection #1 – From Google Canada's cloud data center in Montreal to the Cologix Peering facility in Montreal. This connection will be the responsibility of Shopify.

A Google-managed, Canada-resident fiber connection will connect the Google Canada's cloud data center in Montreal to the Cologix Peering facility in Montreal. In this peering facility, a connection will be made between a Telus fiber network port and the Google-managed fiber connection's network port.

Shopify has confirmed that all information over this connection will be routed through Canada as the connection will fail in the event that the data falls outside of the Canadian sovereign route. To clarify, it will be impossible for any non-Canadian network paths to be used to transmit LDB data on this connection - all data is guaranteed to stay in Canada.

- 2) Connection #2, Part 1 – Cologix Peering facility in Montreal to TELUS' West Coast Communication Office HUB (CO). This connection is the responsibility of Telus.
- 3) Connection #2, Part 2 – The second part of the sovereign route is from TELUS' CO to LDB's MPLS (Multiprotocol Label Switching) Cloud.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

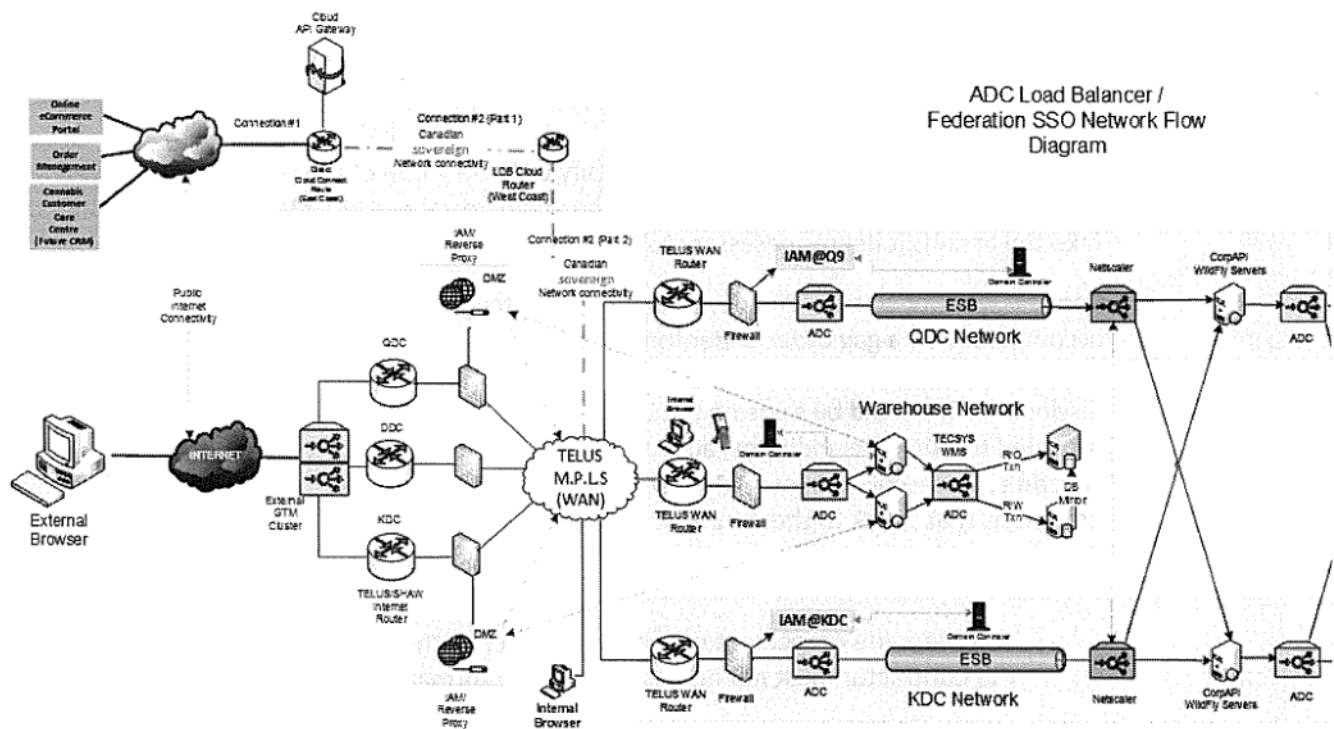
PIA#AG18028

To clarify, the Telus-managed connection will be the carrier of data onward to LDB systems. The LDB currently has a MPLS network with Telus under the current General Service Agreement that Telus or TSSI has with the Province (i.e. Public Service Agency or PSA). Connection #2 (both part 1 and 2) will be an extension of the MPLS network LDB is already running with Telus.

This connection #2 will be a series of joined networks to ensure no non-Canadian network paths are used to transmit LDB data. This is achieved using a series of fiber optic cables and networking equipment.

Data transmitted over these two connections will be encrypted and is unable to be decrypted at any point in the transmission process. Encryption is using a public/private key exchange between LDB systems and Shopify. It is impossible using technology that exists today for this encryption to be broken and the raw data accessed at any point along the network path.

Here is a link to a high level description of the Dedicated Interconnect Overview webpage (<https://cloud.google.com/interconnect/docs/details/dedicated>).





Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Access: General/User

From a logical access perspective, access to LDB information and the systems processing such information requires multi-factor authentication, will be based on role, and will be subject to approval via the automated access broker. This access control will also determine authorization to perform modifications to personal information, and determine access to sensitive information such as encryption keys and other sensitive credentials.

From an unauthorized system change perspective, all application changes will be required to follow the change control process, requiring code review approvals, security review, and successful completion of thousands of automated tests ensuring the integrity of data processed by the system. Developers will not have access to production systems and all code changes will be performed using automated technology.

Access: Legal Compliance

Although highly unlikely, it is conceivable that Shopify may receive a request for information (which may or may not be accompanied by a gag order) by foreign law enforcement (e.g. under FREEDOM Act/FISA Court Order). There are two scenarios that must be considered with respect to legal compliance.

- 1) Request with Notice – In this scenario Shopify will notify LDB of the request for the access to the data before disclosure. LDB will have the ability to contest the disclosure once notified and take the actions it deems necessary to protect the data.
- 2) Request without Notice – In this scenario Shopify may receive a request for information, accompanied by a gag order under foreign law. Shopify will be required to take reasonable steps before complying with such an order, including steps to challenge the compelled disclosure. This could be done on the basis of jurisdiction, in conjunction with other arguments provided through the additional access/disclosure wording in the MSA and Privacy Protection Schedule, as described in number 4, section 9, "Risk Mitigation Table". Below are the contract provisions that speak to these mitigation strategies:

Privacy Protection Schedule, Paragraph 19, 20, 21 and 22:

19. Unless the Agreement otherwise specifies or the LDB otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

20. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the Contractor, the Contractor must immediately notify the LDB.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

In this section, the phrase “unauthorized disclosure of personal information” will bear the same meaning as in section 30.5 of the Act

21. Notwithstanding section 9, if a law enforcement or regulatory authority contacts the Contractor with a demand for access to or disclosure of personal information or LDB Data, the Contractor must promptly advise the authority to make the demand to the LDB and will use best efforts to redirect the authority to make such demand directly to the LDB.

22. If the Contractor is compelled by law to disclose or allow access to personal information or LDB Data, the Contractor will: (a) where permitted by applicable law, provide the LDB with reasonable prior written notice of such compelled disclosure or access; (b) provide the LDB with reasonable assistance if the LDB wishes to contest the disclosure or access; (c) in the case of compelled disclosure or access outside of Canada and notice to the LDB is not permitted by applicable law, take reasonable steps to challenge the compelled disclosure, including presenting evidence at court with respect to: (i) the control of personal information or LDB Data, as the case may be, by the LDB as a “public body” under the Act; (ii) the application of the Act to Contractor as a “service provider” to the LDB that may make such compelled disclosure or access an offence under the Act; and (iii) such compelled disclosure or access being in conflict with the Act; and (d) only disclose or allow access to the minimum personal information or LDB Data necessary to comply with applicable law and in no circumstances provide: (i) blanket or unfettered access to personal information of LDB Data; or (ii) the encryption keys used to secure LDB Data or the ability to break such encryption.; in each case at the cost of LDB but only to the extent any costs are incurred that would not otherwise be incurred as part of Shopify’s standard response to such compelled disclosure or access.

Steady State SOW, Appendix 1, section 2

The e-commerce Solution will comply with the *Freedom of Information and Protection of Privacy Act* (BC), the provisions of Schedule D (Privacy Protection Schedule) to the Agreement and Schedule J (Security Schedule) to the Agreement;



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers PIA#AG18028

License Agreement, section 4.2:

1.1 Termination for Cause

By the LDB: The LDB may terminate this Agreement and the e-commerce Services SOW for cause effective immediately, without payment of any termination fees, penalties, costs or other similar amounts of any kind, upon delivery of a notice of termination to Shopify if: (i) Shopify breaches, in any material respect, any of Shopify's obligations under this Agreement or the e-commerce Services SOW and has not remedied the breach within 45 days after receipt of a default notice from the LDB identifying the breach and stating the LDB's intention to terminate this Agreement and the e-commerce Services SOW if Shopify does not cure the breach within the 45 day cure period; (ii) Shopify breaches Section 10 of the General Terms and Conditions incorporated herein by reference, the Privacy Protection Schedule or Security Schedule; (iii) an Infringement Allegation is made against the LDB and the Shopify SaaS Services, the Support Services or the Shopify IP subject to such Infringement Allegation is determined to have actually infringed, misappropriated or otherwise violated the IP Rights of a third party; (iv) if a termination right set out in the MSA that provides for a specific right of LDB to terminate the MSA or the e-commerce Services SOW occurs and such termination occurs prior to Go-Live; (v) Shopify is bankrupt, insolvent, or unable to discharge Shopify's liabilities as they become due, Shopify commences, maintains or is subject to any proceedings for the benefit of insolvent debtors or for protection from creditors or relating to Shopify's liquidation, dissolution or winding-up or insolvency or the appointment of a receiver, receiver-manager or similar officer or custodian for Shopify or all or any significant part of Shopify's assets or business, Shopify makes an assignment for the benefit of all or substantially all of Shopify's creditors, Shopify suspends or ceases, or threatens to suspend or cease, to carry on Shopify's business in the normal course, or Shopify is subject to any liquidation, winding-up or dissolution; or (vi) Shopify assigns or attempts to assign this Agreement to a third-party in violation of this Agreement

There may also be instances when Google Canada will be compelled by foreign law to provide access to LDB data in order to comply with a legal order. There are two scenarios that must be considered with respect to legal compliance.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

- 1) Request with Notice – In this scenario Google Canada will notify Shopify of the request for the access to the data. Shopify will then notify the LDB. LDB will have the ability to contest the disclosure once notified and take the actions it deems necessary to protect the data.
- 2) Request without Notice – In this scenario Google Canada may be compelled by law to provide LDB's data and not notify the LDB or Shopify that it has done so. Shopify has indicated that, through Shopify's contractual language with Google, that Google before complying with such an order, will take reasonable steps to challenge the compelled disclosure. In addition there are mitigation steps outlined in number 5 of section 9, "Risk Mitigation Table".

Finally, there also may be instances when, for health, safety or emergency purposes, Google US may access LDB data on Google Canada's server. Google has contractual right to access this data under their contract with Shopify. However, this risk is mitigated by the fact that Google has no visibility into the hosting location of a specific shop within Shopify's infrastructure, thus handling a legal request regarding buyer data for a specific client such as LDB is not technically feasible. LDB data is structured such that, even with access to systems containing the information, the LDB attribution of customer data would not be apparent without exceptional technical knowledge of Shopify's systems. Google Canada has thousands of servers across multiple data centres and Google would have no idea where LDB data or even Shopify data can be found across these servers. This will require Google to notify Shopify and Shopify would then notify the LDB, as per the MSA agreement (section 19 of the Privacy Protection Schedule). These measures combine to present an exceptionally low risk of Google having the means, legal authority and/or the technical capability of obtaining LDB's or any other customer's records.

In addition, Shopify has confirmed that disclosure for health, safety or emergency purposes, under Shopify's contract with Google, has never occurred before.

As further mitigating measures, should LDB ever require additional protection to historical data, LDB can also direct Shopify in writing to destroy all personal data held by Shopify as per section 4.4 (h) of the License Agreement between the LDB and Shopify.

All access to data, even if accompanied with a gag order, will be logged at a system level and forms part of the transparency access reports which will be scanned by Shopify systems every 15 minutes. Shopify will be contractually obligated to report any unauthorized access to LDB data to the LDB immediately, as per paragraph 20 of the Privacy Protection Schedule.

In the exceptionally unlikely event that LDB becomes aware through Shopify system monitoring (logs) and notification process that LDB data has been accessed inappropriately, contract language provides for LDB termination rights. To clarify the LDB will have the right to terminate for cause where Shopify breaches any of the confidentiality, privacy and security provisions (i.e. section 10 of the MSA General Terms and Conditions, the Privacy Protection Schedule or Security Schedule).



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers PIA#AG18028

For more information on Google's Transparency Access Reports please visit:

- Google security design:
<https://cloud.google.com/security/https://cloud.google.com/security/>
- Google transparency report:
<https://transparencyreport.google.com/https://transparencyreport.google.com/>

Access: Technical Support Outside of Canada

Tier 1 support requests from e-commerce customers (e.g. customer having trouble logging in, customer forgetting their password or needing help with their order) will be directed exclusively to LDB staff, specifically LDB Customer Care Centre staff or IT Support Centre staff (Tier 1). Any technical issues that cannot be resolved at the Tier 1 level may be escalated by LDB Customer Care Centre staff or IT Support Centre staff to Shopify technical support staff or their technical support subcontractors Pixel Union or Task Us for Tier 2 support. Technical issues that may be escalated to Tier 2 support will include:

- (A) installing, implementing, maintaining, repairing, trouble shooting or upgrading or equipment that includes an electronic system, or
- (B) data recovery that is being undertaken following failure of an electronic system. Some of Shopify's technical support staff as well as all Task Us staff are located outside of Canada. Shopify has call centres in both Canada and outside of Canada (Philippines and Ireland) and Task Us staff are located globally. Tier 2 support from this contractor and subcontractor outside of Canada will be instigated in two ways:
 1. LDB Support staff may call Shopify/Task Us staff outside of Canada if they cannot resolve a technical issue with the system at the Tier 1 level.
 2. In operationally urgent situations, Shopify staff outside of Canada or Task Us staff outside of Canada may instigate Tier 2 support on their own (i.e. without a request from LDB support staff) in cases where they become aware of a technical issue, i.e. the customer database being down.

All Shopify or Task Us staff who support the LDB may be required to access the personal information of LDB customers to resolve technical issues, i.e. Shopify, Pixel Union or Task Us staff may need to access the database where LDB customer PI is stored to identify and resolve technical issues, i.e. to debugging the system.

Temporary access will be granted to Shopify staff outside of Canada and Task Us staff outside of Canada by an automated access broker. To clarify what is meant by "automated access broker",



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

all decisions to grant access to personal information outside of Canada will be governed by an access request evaluation and rules system based on a) identity of the user (i.e. duration of their service at Shopify, completion of training, completion of access request documentation, etc.) and b) the user's device profile (i.e., device security configurations). This access request evaluation and rules system is configured and operated in Canada. This system will maintain the configuration of access control mechanisms protecting access to Personal Information, and will enforce time limitations (i.e. time out session of 15 minutes; a limited amount of times a session can be renewed) on access to Personal Information from outside Canada so that all such access is temporary and complies with this Agreement. If any personnel of Shopify or its subcontractors require temporary access to Personal Information to provide Support Services in accordance with this Agreement for any period beyond the applicable limited period enforced by such system, any such additional access will be granted by Shopify on a manual basis.

As described above, as Tier 1 support requests will be resolved by LDB Customer Care Centre staff or IT Support Centre staff the only requests that will be escalated to Shopify staff outside of Canada and Task Us staff will be authorize by 33.1(1)(p) of FOIPPA, i.e. requests for technical support that include installing, implementing, maintaining, repairing, troubleshooting or upgrading or equipment that includes an electronic system, or data recovery that is being undertaken following failure of an electronic system

Access: Google US access to the data

Google US will not have visibility into LDB customer data on Google Canada's server. To clarify, Google US will not have perpetual access to LDB data on Google Canada's servers. Access to LDB data will only be gained through requesting access through Google Canada. Furthermore, Google Canada will not have visibility into the hosting location of a specific shop within Shopify's infrastructure so there will be a further technical barrier preventing Google Canada from accessing LDB information. Buyer PI data will be structured in such a way that, even with access to systems containing the information, the LDB attribution of customer data would not be apparent without exceptional technical knowledge of Shopify's systems. Google Canada has thousands of servers across multiple data centres and Google would have no idea where LDB data or even Shopify data could be found across these servers. Therefore, both Google Canada and Google US would need to contact Shopify and get their assistance in order to access LDB customer data.

Canada Post systems

Personal information of LDB retail customers will be stored on Canada Post's servers located in Canada and only accessible from Canada.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

8. Personal Information Flow Table

Personal Information Flow Table#1: Retail Customer Ordering			
	Description/Purpose	Type	FOIPPA Authority
1.	A customer who wishes to sign up for an account on the LDB's e-commerce system will be directed to the IAM webpage. As described in Part 1 section 4 above as well as in PIA JAG 15038, age verification will be done and personal information will be collected from retail customers when they fill out the registration page for setting up an account in IAM.	Collection Use	26(c) 32(a)
2.	Customers who sign in as guest will be required to verify their age before entering the e-commerce system. Age verification is automatically calculated by the system using date of birth customer enters. If customer passes age verification step they will be presented with the log-in screen if they have an IAM profile.	Collection Use	26(c) 32(a)
3.	If the customer has an IAM profile, his or her information will be pulled from IAM into the e-commerce platform on first login and access. The e-commerce order will open up with these four fields of information pre-populated from IAM.	Use Disclosure Collection Disclosure (to the individual)	32(a) 33.2(a) and (c) 26(c) and (e) 27(1)(b) 33.1(1)(i.1), 33.1(7)
4.	Customer will be required to enter additional info (order details, billing address, and payment information) to order.	Collection Use	26(c) and (e) 32(a)



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

5.	Payment info will be collected on a separate webpage (which looks seamless to the user) than the order page and all payment information (i.e. credit card information) will be transmitted to TD Bank through their gateway service provider, Bambora/BC Express Pay. The funds go to LDB accounts that are administered by Provincial Treasury, but the government does not transmit or receive the credit card data, which is encrypted immediately after it is entered.	Out of scope of this PIA	n/a
6.	The email addresses of retail customers will be used to send follow up emails on their order, recalls, returns, opportunities to sign-up for promotional materials, etc.	Use Disclosure	32(a) 33.1(1)(i.1), 33.1(7)
7.	The customer's order is transmitted to the LDB's WMS, to be assembled by LDB warehouse staff.	Disclosure Collection Use	33.2(a) and (c) 26(c) and (e) 27(1)(b) 32(a) and (c)
8.	Customer information (shipping address, tracking number) will be transmitted from the LDB systems to the Canada Post systems via SFTP in order for Canada Post to generate a file in its systems for that order.	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a) and (c)
9.	Canada Post employees will arrive at LDB cannabis warehouse to pick up assembled packages. Their business ID will be verified by LDB warehouse staff upon arrival.	N/A	N/A
10.	Label will be scanned in by Canada Post employees and order status will be updated to "Picked Up from Depot" status in Canada Post's systems.	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a) and (c)



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

11.	Canada Post employees will deliver the product to customer address. If the retail customer is present at address to receive package, Canada Post employees will request to see customer's government issued ID for age verification, if the customer appears to be under 25 years of age. Customer's signature will be collected electronically by handheld device and label will be scanned into the Canada Post systems to update the status to "Delivery Successful".	Use Disclosure Collection Use	32(a) and (c) 33.2(a) 26(c) 32(a)
12.	Confirmation that package was successfully delivered to customer will be sent to LDB via SFTP. The information will be used to update the LDB systems.	Disclosure Collection Use	33.2(a) and (c) 26(a) 27(1)(b) 32(a) and (c)
13.	Individual customer orders are used to gather statistics (i.e., most popular products or top products in X city in BC).	Collection Use	26(e) 32(a)

Personal Information Flow Table #2 - Return to Sender

	Description/Purpose	Type	FOIPPA Authority
1.	If the attempt to deliver the package to the customer by Canada Post is not successful (i.e. no such address found, customer refuses delivery), Canada Post employees will make note of it, advise LDB and return the merchandise to LDB's cannabis warehouse.	Collection Use Disclosure	26(c) 32(a) 33.2(a) and (c)
2.	LDB Warehouse employees will scan the product back into the LDB inventory and note the reason for return in WMS.	Collection Use	26(c) 27(1)(b) 32(a) and (c)



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Personal Information Flow Table #3 - Drop off of Customer Order at Canada Post Depot			
	Description/Purpose	Type	FOIPPA Authority
1.	In cases where no one is present to receive and sign off for the package, Canada Post employees will leave a Delivery Card Notice (DNC) adhered to customer door which states that the package will be dropped off at the nearest Canada Post Office.	Disclosure	33.2(a)
2.	Customer will take the DNC and go to nearest post office to pick up the package.	N/A	N/A
3.	At the Post Office, the Canada Post employee will check the DNC of the customer, verify the government issued photo ID, and ensure that the address on the customer's ID matches the address on the package.	Collection Use	26(c) 32(a)
4.	If the address on the customer's ID matches, the customer will be allowed to sign for the package and receive package.	Collection	26(c)
5.	If the customer does not come to pick up the package at the Canada Post depot within 15 days of the DNC being delivered, the package will be sent back to the LDB cannabis warehouse where LDB employees will scan the package into WMS to adjust the inventory.	Use Disclosure Collection Use	32(a) 33.2(a) and (c) 26(c) 32(a) and (c)

Personal Information Flow Table#4 – Technical Support			
	Description/Purpose	Type	FOIPPA Authority
Tier 1 - Inside Canada			
1.	LDB Customer Care Centre staff or LDB IT Support Centre staff receive request from e-commerce customer and resolve issue.	Out of scope of the PIA	n/a



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Tier 2 - For technical issues that cannot be resolved at Tier 1 level			
2.	LDB Customer Care Centre staff or IT Support Centre staff will request support from Shopify's Call Centres inside of Canada or Pixel Union.	n/a	n/a
3.	Shopify's Support staff inside of Canada or Pixel Union staff determine that they need to access LDB's customer database to resolve the issue.	Disclosure [LDB] Collection [Shopify and Pixel Union] Use [Shopify and Pixel Union]	33.2(a) and (c) 26(c) 27(1)(b) 32(a) and (c)
4.	In some cases the technical support may come from Shopify's Support staff outside of Canada or TaskUs staff	Disclosure [LDB] Collection [Shopify and TaskUs] Use [Shopify and TaskUs]	33.1(1)(p) 26(c) 27(1)(b) 32(a) and (c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	LDB and Shopify/Task Us/Pixel Union employees (i.e. Customer Care Centre staff) could access personal information on the e-commerce system and use or disclose it for unlawful personal purposes.	<ul style="list-style-type: none"> Oath of Employment for LDB Standard of Conduct for LDB Privacy training for LDB employees and contractors and technical support contractors who have access to LDB databases. Role-based access Criminal background checks for LDB employees and security screening for Shopify employees. The LDB will follow the security requirements set-out by PSSG- enhanced security 	Low	High

For PCT Use Only:
Version 1.0



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

		<p>clearances for anyone directly related to the Cannabis line of business - this will include anyone who has access to the e-commerce system and integrated systems.)</p> <ul style="list-style-type: none"> • Shopify and subcontractors are bound by contract with LDB 		
2.	Request may be from a minor (i.e. a minor may login to the client's account or may misrepresent themselves as a person over 19).	Consumers will be asked to input their DOB into the website before they can order any product. If they input a DOB that calculates below the age of 19 they will not be allowed to proceed to the ordering page. In addition there will be an additional Photo ID verification by Canada Post at the time of delivery, to verify if the customer receiving the package is over 19.	Low	High
3.	Client's personal information is compromised by security breach or cyber-attack when transferred to Shopify.	See section 12 of the PIA.	Low	High
4.	Google US or Google Canada staff unlawfully access LDB customer data at rest on Shopify's servers with Google encryption keys.	<p>The LDB is satisfied that the contractual mechanism (i.e. Shopify License Agreement and Steady State SOW) provides the appropriate risk mitigation, including contractual remedy should Shopify breach its obligations and allow unauthorized access to the data outside of lawful and emergency based requests.</p> <p>In addition, all unauthorized access to data, even if accompanied with a gag order, is logged at a system</p>		



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

		<p>level and forms part of the transparency access reports which are contractually provided to Shopify by Google on a regular basis and Shopify will be verifying through an automated process every 15 minutes. Shopify will immediately notify LDB of any authorized access found through these reports within 1 hour of discovery if the access is for purposes of complying with a lawful request and within 24 hours for authorized access via a security breach as per Appendix J of the contract, Security schedule. Access logs will not be provided to the LDB.</p> <p>Lastly Google would need to engage Shopify to identify/locate data OR Google would need to access all of Shopify's data (including Province data), which is functionally highly difficult given the volume of data and an overly broad data collection process in response to a compelled disclosure request. Google Canada has thousands of servers across multiple data centres and Google would have no idea where LDB data or even Shopify data can be found across these servers and data centres.</p>		
--	--	---	--	--



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

5.	Shopify receives a lawful request for the Province's data from a foreign or legal body and by law are NOT permitted to inform the Province.	<p>The LDB is satisfied that the contractual mechanism (i.e. Shopify License Agreement and Steady State SOW) provides the appropriate risk mitigation, including contractual remedy should Shopify breach its obligations. Specifically Shopify would deny all foreign demands as they are unauthorized and would be willing to fight the disclosure in court should it be unauthorized.</p> <p>An overly broad data collection process in response to a compelled disclosure request would place Google Canada in violation of their contractual agreement with Shopify.</p>	Low	High
6.	Google Canada receives a lawful request for the LDB's data from a foreign or legal body and by law is NOT permitted to inform Shopify or Province.	<p>Google would need to engage Shopify to identify/locate data OR Google would need to access all of Shopify's data (including Province data), which is functionally highly difficult given the volume of data and an overly broad data collection process in response to a compelled disclosure request. Google Canada has thousands of servers across multiple data centres and Google would have no idea where LDB data or even Shopify data can be found across these servers and data centres.</p> <p>Shopify has agreed, in contractual language of the MSA (Privacy Protection Schedule), to deny all foreign demands as they are unauthorized and would be willing</p>	Low	High



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

		<p>to fight the disclosure in court should it be unauthorized.</p> <p>In addition, all access to data, even if accompanied with a gag order, is logged at a system level and forms part of the transparency access reports which are contractually provided to Shopify by Google on a regular basis and Shopify will be verifying through an automated process every 15 minutes. Shopify will immediately notify LDB of any authorized access found through these reports within 1 hour of discovery the access if for purposes of complying with a lawful request and within 24 hours for authorized access via a security breach as per Appendix J, Security schedule, although access logs will not be provided to the LDB.</p> <p>An overly broad data collection process in response to a compelled disclosure request would place Google Canada in violation of their contractual agreement with Shopify.</p>		
7.	<p>Google receives a request for the LDB's data for health, safety or emergency purposes and, under Shopify's contract with Google, Google has contractual right to access this data.</p>	<p>Google would need to engage Shopify to identify/locate data OR Google would need to access all of Shopify's data (including Province data), which is functionally highly difficult given the volume of data and an overly broad data collection process in response to a compelled disclosure request. Google Canada has thousands of servers across multiple data centres and Google</p>	Low	High



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

		<p>would have no idea where LDB data or even Shopify data can be found across these servers and data centres.</p> <p>Shopify would be required to notify the Province before the disclosure has been made, as per the MSA (paragraph 19 of the Privacy Protection Schedule</p> <p>In addition, all access to data is logged at a system level and forms part of the transparency access reports which are contractually provided to Shopify by Google on a regular basis and Shopify will be verifying through an automated process every 15 minutes. Shopify will immediately notify LDB of any unauthorized access to LDB records found through these reports within 1 hour of discovery the access if for purposes of complying with a lawful request and within 24 hours for authorized access via a security breach as per Appendix J, Security schedule, although access logs will not be provided to the LDB.</p> <p>Shopify has also stated that disclosure for health, safety or emergency purposes and, under Shopify's contract with Google, has never occurred.</p>		
8.	Access to the LDB personal data outside Canada under the "follow the sun" support model - Shopify's staff outside of Canada or Task Us staff will have access and	Under contract, Shopify and Task Us staff should only access personal information outside of Canada when it would be authorized by s. 33.1(1)(p) of FOIPPA. As LDB's Support Centre	Low	High



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

	<p>the ability to cause data to leave Canada on a temporary basis.</p>	<p>and Customer Care Centre will handle all Tier 1 support calls from customers, all inquiries that will be escalated to Tier 2 are technical issues that cannot be resolved internally, i.e. installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system or equipment that includes an electronic system, or data recovery that is being undertaken following failure of an electronic system.</p> <p>Risk of unauthorized access is mitigated through access controls and contractual mechanism (i.e. Shopify MSA and Privacy Protection Schedule).</p> <p>In addition, Shopify has confirmed that support staff outside of Canada (i.e. Shopify staff and Task Us staff) will not be given standing access to LDB data- rather temporary approval via an automated access broker in Canada will ensure access to support staff outside of Canada is temporary.</p> <p>Shopify has also confirmed that all of its IT support staff who have access to LDB customer data (i.e. Shopify call centre staff, Pixel Union staff and Task Us staff) will be required to take either Shopify's privacy training course (content deemed equivalent to BC government training) or the course offered by the BC government.</p>		
--	--	--	--	--



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

9.	Proper flow-through privacy requirements from government to Shopify's sub-contractor.	Shopify has confirmed in writing that Shopify's contractual terms with Google do not contradict any of the terms in the MSA, Privacy Protection Schedule and Security Schedule of their contract with the LDB.	Low	High
10.	Retention and destruction of customer data.	The LDB is satisfied that the contractual mechanism (i.e. Shopify MSA and Privacy Protection Schedule) will mitigate this risk. Shopify has agreed in writing to destroy all LDB customer data past 8 years of retention. In addition, they have confirmed, as per section 4.4(h) of the License Agreement that should LDB request in writing that all LDB customer personal information be deleted from Google's servers that Shopify has the ability to do so.	Low	High
11.	Customer order may be mislabelled and personal information shipped to the wrong person.	Warehouse shipping procedures will ensure standardized processing of orders Training on warehouse procedures	Low	Medium
12.	Shipments may be lost, intercepted, or mishandled en-route to consumer.	Use of a trusted delivery service provider (i.e. Canada Post).	Low	Medium
13.	Personal information is compromised when transferred from LDB's e-commerce platform to the WMS.	Technical security measures (See Part 3)	Low	High



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

14.	Personal information is compromised when transferred from LDB's WMS to Canada Post	Information is encrypted and securely transmitted through SFTP.	Low	High
-----	--	---	-----	------

10. Collection Notice

Retail customers who opt to create an IAM account will be given the following notice:

"The Liquor Distribution Branch is collecting your personal information to manage your user identity and access permissions for LDB applications and to receive, process, and send your orders for delivery. This information is being collected pursuant to section 26(c) and 26(e) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of your personal information please contact the Manager of Information, Privacy, and Access, BC Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3043"

All retail customers who visit the e-commerce website are asked to input their DOB to enter the e-commerce website will be given the following notification:

Your DOB will be used to ensure you meet the age (19+) requirements when you enter our e-commerce website. Your DOB is being collected pursuant to section 26(c) of the Freedom of Information Protection of Privacy Act but will not be stored in our systems. For any questions regarding the collection please contact the Manager of Information, Privacy, and Access, BC Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3004.

All retail customers who submit orders on the e-commerce website will be given the following notice on the e-commerce online order form:

"The Liquor Distribution Branch is collecting your personal information (i.e. contact details and order information) in order to process your cannabis order, to send you updates on your order via email and to evaluate our e-commerce platform. We may also use your email address to contact you about recalls and future opportunities to receive promotional materials. This information is being collected pursuant to section 26(c) and 26(e) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of your personal information please contact the Manager of Information, Privacy, and Access, BC Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3043"

(Tickbox) to "I have read and understood the privacy policy and I authorize LDB to communicate with me via email."



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Part 3 – Security of Personal Information

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

Shopify:

Facilities where data will be stored by the service provider are ISO 27001, PCI DDS, and SOC2 compliant and undergo regular onsite audits to validate the security controls.

More details can be found in the SOC 2 Report.

LDB:

Physical security measures for the warehouse building are as follows:

- High security locks and keys
- Perimeter gate controls
- Key card required for access. Each key card is associated with a specific employee and access swipes are logged and auditable
- 24/7 surveillance in warehouse building and on exterior of building
- 24/7 security personnel on-site
- Locked cabinets for shipping lists and un-affixed labels
- After-hours alarm system which notifies security and police in the event the alarm is triggered

LDB:

The Non-Medical Cannabis Wholesale Supply Chain initiative will store personal information in the WMS in the form of customer orders. The WMS system is located on LDB servers and the LDB servers are kept in a locked building. Access to the building is only possible to employees with a key card, or to guests who have signed in at reception and are accompanied by an employee.

Physical security measures for the warehouse building are as follows:

- High security locks and keys
- Perimeter gate controls
- Key card required for access. Each key card is associated with a specific employee and access swipes are logged and auditable
- 24/7 surveillance in warehouse building and on exterior of building



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

- 24/7 security personnel on-site
- Locked cabinets for shipping lists and un-affixed labels
- After-hours alarm system which notifies security and police in the event the alarm is triggered

Canada Post physical security measures

- High security locks and keys
- Perimeter gate controls
- Key card required for access. Each key card is associated with a specific employee and access swipes are logged and auditable
- 24/7 surveillance on exterior of building
- 24/7 security personnel on-site
- Locked cabinets for confidential information
- After-hours alarm system which notifies security and police in the event the alarm is triggered
- A dedicated team of Postal Security Officers and a team of Postal Inspectors that are recognized as an investigative body
- Strict visitor management process
- Restricted access that is granted on an as-needed basis and only after the issuance of a Reliability Security Screen of new employees and contractors (involving the use of fingerprints)

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

Shopify:

Shopify encryption keys will be used on LDB data in transit and Google does not have access to these encryption keys (only Shopify has access to these encryption keys). Google encryption keys will be used on data at rest.

The service provider uses numerous methods to ensure the security of the information and the system that holds it. Information in transit is encrypted using industry-standard cryptographic protocols:

- SSH
- IPSec
- HTTPS-TLSv1.2



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

All transactional data is encrypted in transit and at rest in operational data stores. Shopify will rely on its own encryption for data in transit and Google encryption for data at rest.

The service provider's application security team implements automated controls for all types of systems used in the provision of the service, including dependency vulnerability monitoring, data isolation testing, static analysis, code signing, and kernel hardening. Furthermore, developers are trained regularly on application security best practices, including OWASP Top Ten. An automated service running on the service provider's code base monitors application dependencies for vulnerabilities. If a security issue is discovered in a library, developers respond quickly to mitigate any risk.

Customer input, such as form fields, is validated against a whitelist and decoded safely. Input validation and decoding protect against common attack vectors, including:

- HTML injection
- SQL injection
- XSS

Server and application performance is monitored continuously by a production engineering team. Performance metrics are established for numerous aspects of the service, such as response time, network throughput, application exceptions, and other service-oriented metrics for critical components. Production engineering, security operations, and many other teams within the organization operate a 24/7 paging service to ensure prompt attention to any detected abnormalities in system operations.

Configuration management tools ensure servers have the current configuration applied. Hourly applicable security patches are installed on all servers. Production users are authenticated by public key authentication. Access is granted by configuration management and role-based access controls at the network perimeter.

LDB Servers:

- Robust network security architecture including firewalls
- Encryption of all data in transit
- Individual accounts for all access to data. (i.e. no generic accounts)
- Full Audit Log of system activities



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Canada Post:

Canada Post has adopted an extensive information security and risk management program based on recognized industry standards and best practices to protect our IT assets and our data. Security measures include:

- Firewalls;
- Encryption – of data at rest and in transit;
- Anti-virus software;
- Vulnerability scanning;
- Penetration testing;
- Patch management;
- Change management;
- Access controls;
- Multifactor authentication (for remote access);
- Physical controls;
- Audit trails;
- SIEM; and
- IDS / IPS.

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

Shopify:

Shopify does maintain a set of internal IT Security policies. These policies are compliant with PCI DSS policies.

LDB:

LDB has its own Information Security Policy. It is based on the government's Information Security Policy, based on ISO 27001. The policy is consistent with government and has been adapted for the LDB environment. The contract with Shopify included a Security schedule (Schedule J), which ensures Shopify meets government's Information Security Policy.

Canada Post:

Canada Post relies on a broad set of internal security policies that are informed by industry standards such as ISO (27001 / 27002), ITSG-33, and PCI DSS.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

14. 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.

Shopify:

Shopify's application can be configured to set role-based access levels which are controlled by multi-factor authentication for staff log-in.

From a logical access perspective, access to LDB information and the systems processing such information requires multi-factor authentication, is based on role, and is subject to approval via the automated access broker. This access control also determines authorization to perform modifications to personal information, and determines access to sensitive information such as encryption keys and other sensitive credentials.

From an unauthorized system change perspective, all application changes must follow the change control process, requiring code review approvals, security review, and successful completion of thousands of automated tests ensuring the integrity of data processed by the system. Developers do not have access to production systems and all code changes are performed using automated technology.

LDB:

Data is restricted to role-based access. To clarify personal information will only be accessed by Assemblers, who will receive it from the WMS. Editing privileges will be restricted to the e-commerce system (with information flowing to the WMS) and will only be granted to the customer themselves or to Customer Care Centre employees (see Customer Care Centre PIA).

All internal LDB users with valid credentials will have the ability to authenticate to the WMS. Their user name and password to LDB systems will authenticate them in the WMS.

Only users who have a business reason to view documents with personal information will be granted access to them, as per their role.

Canada Post:

From an access control perspective, see below.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Role-based	Yes
Permission-based	Yes
Logging of views / updates	Yes

Other controls that mitigate the risk of unauthorized change include:

- Change management
- File integrity monitoring (FIM)
- Vulnerability scanning
- Penetration testing
- Others

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

Shopify:

Logs are created of the following events:

- Web requests processed by Shopify
- Server activity
- Application activity
- Log access activity
- Authentication attempts

Logs are kept on log servers for approximately one month. They are then moved to off-site backup locations, where they remain available for 12 months.

LDB:

Access to data is logged and logs will be auditable.

Shipping lists and labels will only be generated by Assemblers. Labels that have been affixed to packages will be kept in areas monitored by video surveillance. Onsite security will monitor cameras and gate control.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Canada Post:

Access to and modification of personal information will be logged.

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. 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?**

Updating and correcting personal information will happen through the e-commerce platform, and will be disseminated to the WMS accordingly. Retail customers will have the ability to login to their accounts to update their own information, if they choose to have a permanent account. Permanent account holders and guest customers will also have the contact the Customer Care Centre via telephone and email to request a change. Business to business clients will be required to call the Customer Care Centre (Business to business information will not include personal information).

Canada Post:

There will be no ability for customer contact information to be updated once the package is sent by courier.

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

Yes. Customers will be providing an attestation that they are 19 years or older, and their ability to access the services will be based on this assessment. Furthermore, the name and/or delivery address of consumers will be verified to collect packages from post office locations if no one is available to receive it when delivery is attempted.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

Prior to submitting an order, the consumer will be asked to verify the information that has been provided by the consumer for order processing.

Canada Post delivery employees will verify government-issued photo ID of any customer who appears to be under the age of 25 to confirm that the person receiving the package is over 19.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

If the retail customer is picking up the package at a Canada Post Office, Canada Post will check their:

- Their delivery notice card
- Government-issued photo ID

If the customers are unable to pick up the item themselves, they will have the ability to send someone else in their place. The representative will be required to bring government-issued photo ID and one of the following:

- The delivery notice card. The customer must sign the card and print the name of the person they have sent to pick up the item on their behalf, or
- A letter of authorization or a legal document demonstrating their authority to act on the customer's behalf.
- Post office staff will verify that the customer's address matches the address of the package.

19. If you answered "yes" to question 17, 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?

There is a proposed records retention schedule that has not yet been approved. No records will be destroyed until the records schedule is approved. The proposed records retention schedule will require LDB to retain customer order information 7 years after the transaction has been completed. The vendor, Shopify, has proposed that records may be anonymized 180 days after the transaction has been completed to provide sufficient time to process refunds or credit card disputes that might affect an order. However, any instruction to the vendor in this regard will only be made in accordance with the approved records retention schedule.

Part 5 – Further Information

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

Yes, there is systematic sharing of information between the service providers and LDB. However, the service providers are defined as an employee of LDB as per Schedule 1 of FOIPPA and as such there is no requirement to develop an information sharing agreement when information is shared within a public body for a consistent purpose.



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

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

No.

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

Yes. Customers' orders will be searchable by name or order number and customers who create permanent accounts will be searchable. Additionally, shipments will be given tracking numbers on hand-off to carrier, which will be linked to consumers and the WMS will enable an authorized person to access all of the activity of an individual based on their name or user ID.

Personal Information Bank – Required Information	
Description	Contact information for customers and order details will be kept in the database containing accounts and product orders. Customers will be searchable by name, order number, and account ID.
Primary ministry/government agency involved	Ministry of the Attorney General, Liquor Distribution Branch
All other ministries/government agencies and public bodies involved	None
Business contact title	Manager of Information, Privacy, and Access
Business contact telephone number	604 252-3011
Personal Information Bank – Required Information	
Description	Shipments tracking numbers on hand-off to carrier, which will be linked to consumers.
Primary ministry/government agency involved	Ministry of Attorney General BC Liquor Distribution Branch
All other ministries/government agencies and public bodies involved	None
Business contact title	Director of Distribution
Business contact telephone number	604-252-3129



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers PIA#AG18028

Part 6-PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Rhianna Begley

October 15, 2018

a/Director
Privacy, Compliance & Training Branch
Corporate Information & Records
Management Office
Ministry of Citizens' Services

Signature

Date

Matt Reed

October 16, 2018

Executive Director
Privacy, Compliance & Training Branch
Corporate Information & Records
Management Office
Ministry of Citizens' Services

Signature

Date



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers PIA#AG18028

Part 7-Program Area Comments and Signatures

Karlne Bordua

October 16, 2018
Date

Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General

Signature

October 17, 2018
Date

Ian Bailey

Assistant Deputy Minister and Chief
Information Officer
Information Systems Branch
Ministry of Attorney General

Signature

Amin Nanji

Director, Information Technology
Enterprise Solutions
Liquor Distribution Branch
Ministry of Attorney General

Signature

2018/10/23
Date

Michael Tan

Executive Director Cannabis
Liquor Distribution Branch
Ministry of Attorney General

Signature

Date

Blain Lawson

CEO and General Manager
Liquor Distribution Branch
Ministry of Attorney General

Signature

10/29/18
Date



Privacy Impact Assessment for Cannabis E-Commerce Retail Customers

PIA#AG18028

Appendix A: Glossary of Terms:

- **BC Express Pay/Bambora:** BC Government approved online payment portal. Used by government ministries to receive payment by credit card from members of the public for BC government supplied goods and services.
- **Identify Access Management (IAM) system:** IAM is the access system used to control and verify all user system access. Cannabis wholesale customer must set up an account and password as part of their e-commerce registration process. Cannabis retail e-commerce customers also have the option of setting up a user account in IAM for convenience with future online purchases (as opposed to signing in as a guest each time and having to fill in their name and address for each purchase). IAM is an application housed on LDB servers in Canada.
- **Warehouse Management System (WMS):** WMS used by the Cannabis Distribution Center to track and control all incoming and outgoing inventory. All data on WMS will be kept on LDB servers in Canada.



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

Part 1 – General

Name of Ministry:	Ministry of the Attorney General, Liquor Distribution Branch		
PIA Drafter:	Manager, Information, Privacy & Access		
Email:	Manami.Calvo@bcldb.com	Phone:	604 252-3000
Program Manager:	Kevin Satterfield, Director, Cannabis Retail		
Email:	Kevin.Satterfield@bcldb.com	Phone:	604 252-3772

1. Description of the Initiative

Under the oversight of the Ministry of the Attorney General, the BC Liquor Distribution Branch (LDB) is responsible for the purchasing, import, wholesale pricing, distribution and transportation of beverage alcohol in British Columbia (BC). On December 5, 2017, LDB was also tasked with providing non-medical cannabis wholesale and distribution services to the province. In addition, on February 5, 2018, LDB was given responsibility for retailing non-medical cannabis, alongside private retail stores. The *Cannabis Distribution Act* outlines LDB's role and responsibilities in wholesaling, retailing and distributing non-medical cannabis.

To meet the retail mandate of the legislation, LDB is opening BC Cannabis Stores (BCCS) and launching an e-commerce platform that will allow its retail customers to purchase non-medical cannabis (retail customers is defined as individual consumers who will purchase non-medical cannabis either through LDB's e-commerce platform or LDB's brick and mortar stores).

Customer expectations and best practices require that customers have the option of returning or exchanging cannabis products purchased from LDB. Returns will be accepted at BCCS when legitimate circumstances require such a return. LDB has put in place a return policy (see Appendix A) that outlines how and under what circumstances retail customers can return or exchange their purchased products at any BCCS store.

2. Scope of this PIA

This PIA will assess the privacy implications of the process by which cannabis customers return products to BCCS stores.

Note that the processes related to returns through LDB's Customer Care Centre (CCC), the processes related to the "Return to Sender" returns, when Canada Post returns product to the LDB warehouse without having delivered it to the customer and the financial information flow involving the Ministry of Finance Express Pay 2.0/Bambora involved in this process, are outlined in separate PIAs (see below) and will be out of scope of this PIA.



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

3. Related Privacy Impact Assessments

JAG15038 - Identity Access Management

AG18028 – E-Commerce Platform

AG18030 – LDB Cannabis Wholesale and Distribution

SBRT16006 – Customer Returns (Liquor)

AG18039 – Interim Cannabis Customer Care Centre

FIN15017 – BC Express Pay (BCEP) 2.0 Lite-Banking and Cash Management hosted by Beanstream (Beanstream has been renamed Bambora, and will be referred to as Bambora throughout this PIA)

FIN12020 – BC Express Pay-Banking and Cash Management

SBRT16005 – LDB Retail Sales Tracking and Reporting

SBRT16006 – LDB Customer Returns

4. Elements of Information or Data

Personal Information:

When a customer makes a return, the following personal information will be collected directly from the customer by the non-medical cannabis retail store employee in order for the Customer Care Centre to complete a Return Merchandise Authorization (RMA).

- Age verification (through the verification of government issued ID)
- Customer first name
- Customer last name
- Customer address
- Customer phone number
- Customer email
- Reason for return
- Description of why product is returned (free field)
- Order number
- Purchase quantity
- How the payment was made



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

Business (sales) Information:

- Date/Time of transaction
- Transaction number
- Store number
- Register number
- Cashier code (equivalent to userID or Outlook alias)
- Type of purchase
- Tender type
- Transaction total
- Till number
- Transaction status
- Product code
- Product Description

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be stored on LDB servers located in Canada and only accessed from Canada.

6. Data-linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a



Privacy Impact Assessment for LDB BC Cannabis Store Return Process PIA#AG18040

7. Common or Integrated Program or Activity*

In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act.

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

For returns due to product recalls, the following steps will precede the return of the product at the government cannabis stores:

Personal Information Flow Table – Product Recall Notification			
	Description/Purpose	Type	FOIPPA Authority
1.	If a product is recalled, a recall notice will be posted on BCCS website.	n/a	n/a
2.	In the future, LDB may send a recall notice to specific customers who have purchased product. This would apply to customers whose contact information has already been collected at the time of purchase (i.e. E-Commerce).	Use Disclosure	32(a) 33.2(a) 33.1(7)
3.	Customers may contact LDB with questions or concerns.	Collection Use	26(c) 32(a)



Privacy Impact Assessment for LDB BC Cannabis Store Return Process PIA#AG18040

Personal Information Flow Table – Returns Process			
	Description/Purpose	Type	FOIPPA Authority
1.	Customers who appear to be under the age of 30 will be asked to present government issued photo ID upon entering a BCCS. No information regarding ID will be noted down but a decision will be made as to let them enter the store based on the DOB on their ID. .	Collection	26(c)
2.	Customers will present product they want to return at the store.	Collection	26(c)
3.	BCCS employees will verify one of the 4 return criteria is met (see policy Appendix A).	Use	32(a)
4.	BCCS employees will collect customer's personal data elements to fill out an RMA form. The information will be entered in the store's Point of Sale (POS) system by BCCS employees.	Collection Use	26(c), 26(e) 32(a)
5.	If customer paid by cash, a cash refund will be issued to them. If customer's original form of payment was by credit card or debit card, their card will be swiped into the POS central system to issue refund. The financial information flow in the context of returns will be transmitted to TD Bank through their gateway service provider, Bambora/BC Express Pay. The funds go to LDB accounts that are administered by Provincial Treasury, but the government does not transmit or receive the credit/debit card data, which is encrypted immediately after it is entered. This process was previously assessed in FIN15017.	Out of Scope of the PIA	n/a
6.	BCCS staff will send the RMA form to CCC and CCC Return will process the return.	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a)



Privacy Impact Assessment for LDB BC Cannabis Store Return Process PIA#AG18040

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes.	Oath of Employment LDB Code of Conduct BC Public Service Agency Standards of Conduct Privacy Training	Low	High
2.	Client's personal information is compromised when transferred to from BCCS to CCC.	Personal information will be transferred internally to LDB through system integration, by using the BC Government Exchange Web Services (EWS) system email infrastructure or by phone. When it comes to transfer of personal information by email, note that the information will be shared within BC Government infrastructure and the personal information will be encrypted in transfer.	Low	Med

10. Collection Notice

The privacy policy on the BCCS website will state the following:

"A limited amount of your personal information is recorded when you use your debit or credit card to pay for your purchase and when you return product. While you are outside the entrances of our store or inside the store, your image may also be captured by customer awareness cameras. For further information about the collection and use of your personal information, please contact Information, Privacy and Access services at the Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3043.

Secondly a notification about the following collection of customer personal information will be posted at the customer service desk of BCCS stores:



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

"BC Cannabis Stores may collect your personal information under section 26(c) and 26(e) of the Freedom of Information and Protection of Privacy Act to assist with product selection, purchase and product return. For questions about this collection please your store manager or call or write our Privacy Officer at 604 252-3043 or 2625 Rupert Street, Vancouver BC, V5M 3T5. "

All retail customers who submit orders on the e-commerce website will be given the following notice on the e-commerce online order form:

"The Liquor Distribution Branch is collecting your personal information (i.e. contact details and order information) in order to process your cannabis order, to send you updates on your order via email and to evaluate our e-commerce platform. We may also use your email address to contact you about recalls and future opportunities to receive promotional materials. This information is being collected pursuant to section 26(c) and (e) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of your personal information please contact the Manager of Information, Privacy, and Access, BC Liquor Distribution Branch, 2625 Rupert Street, Vancouver BC, V5M 3T5 or call 604-252-3043"

Part 3 – Security of Personal Information

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

The servers hosting the Retail Sales Customer Returns application reside in LDB Data Centres that have strong physical security. The data centres reside in buildings that are monitored physically and/ or electronically (i.e. cameras and alarms) around the clock by Corporate Loss Prevention (CLP) Building Security Officers. Access to the data centres is restricted to staff needed to support the IT infrastructure, first aid staff, and building security officers through a card key system managed by CLP.

The personal information stored as email in the EWS System is stored on BC Government Canadian servers.

The BC Government data centres have 24 hour security and access to the buildings and floors is protected by a door access system run by corporate security. The facilities are surrounded by chain link and barbed wire and access by motorized vehicles.¹⁵

s.15



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

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

The Retail Sales Customer Returns infrastructure is securely configured in accordance with Branch IT Security policies and industry best practices. Independent vulnerability assessments have been performed prior to implementation to confirm significant system vulnerabilities are not present. Periodic vulnerability assessment scans will be performed and significant vulnerabilities identified will be remediated.

Access to the Retail Sales Customer Returns component is restricted to LDB staff with authority, and IT Support users. They must be physically present within LDB premises or if remote, log into the LDB network to access the system. These staff and users must authenticate themselves (i.e. user ID and password) before they are allowed to access the network. Two-factor authentication is present when remotely accessing the LDB network. Staff and users must also provide the authentication code provided by the RSA SecureID token that they have been assigned. Staff and user access to the network is managed in accordance with LDB IT Security policies and procedures.

Only LDB devices that have been configured and maintained (e.g. anti-malware and Internet filtering) according LDB IT security policies can access the system.

In the context of email, the EWS system is only accessible through a valid BC government user ID (IDIR) and password.

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

LDB IT Security Policies are based on and is consistent with government's Information Security Policy. The LDB follows government information policies (i.e. privacy and records retention).

14. 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.

Only store employees are provisioned with the access needed to process customer returns in the POS. Store manager or designate must review and approve the transaction. Access to the information in the finance systems is restricted to appropriate LDB persons for reviewing/editing the transaction.

Security policies have been defined, reviewed, and approved by the business owners of each system. Processes have been defined to ensure appropriate persons are provisioned with the access defined in the security policies.



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

Staff and users must authenticate themselves through passwords before they can access the systems. Access to the applications used to support the Retail Sales Customer Return process is based on roles and responsibilities.

In the context of email, the EWS system is only accessible through a valid BC government user ID and password.

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

POS logs which users have viewed or edited information and what changes have been made.

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
 - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.
- Message Transport logs include message tracking (Exchange server to Exchange server internal only) which provides a detailed record of message activity, such as sent, received date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.
- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. 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 a customer needs to update or correct their information they can contact CCC or go back to the store where they made their return and let them know of the changes.

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

Yes, the personal information is used to determine whether a return is issued.



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

18. If you answered “yes” to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

The product and receipt are checked against the LDB systems.

19. If you answered “yes” to question 17, 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?

LDB has an 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.

Part 5 – Further Information

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

No.

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

No.

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

No, the related PIBs are mentioned in previous PIAs.



Privacy Impact Assessment for LDB BC Cannabis Store Return Process

PIA#AG18040

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Chris Quon
Privacy Advisor
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services



Signature

October 15, 2018

Date

Rhianna Begley
A/Director
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services



Signature


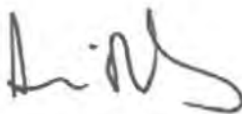


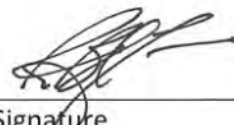
October 15, 2018

Date



Privacy Impact Assessment for LDB BC Cannabis Store Return Process PIA#AG18040

Part 7 – Program Area Comments and Signatures

Karine Bordua Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	 _____ Signature	October 16, 2018 _____ Date
Ian Bailey Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	 _____ Signature	October 17, 2018 _____ Date
Kevin Satterfield Director, IT Business Systems Liquor Distribution Branch Ministry of Attorney General	 _____ Signature	Nov 8 2018 _____ Date
Gary Kuromi LDB IT Security Manager Liquor Distribution Branch Ministry of Attorney General	 _____ Signature	Nov 8, 2018 _____ Date
R. Blain Lawson General Manager and CEO Liquor Distribution Branch Ministry of Attorney General	 _____ Signature	11/9/18 _____ Date



Privacy Impact Assessment for LDB BC Cannabis Store Return Process PIA#AG18040

Appendix A: Cannabis Customer Retail Returns Policy

1. All sales of cannabis product or accessories from BCCS retail (stores and online) shall, except in those circumstances defined and exempted by this policy, be considered final.
2. The four exempted products are:
 - a) Defective Product (Opened cannabis product or accessory which is not fit for use or consumption. In the case of cannabis this could include any mould, fungus, or other foreign contaminant on the cannabis; or staleness. In the case of cannabis accessories this would include, damage that was not identifiable at the time of purchase, or mislabelling)
 - Shall be accepted for return and refund, provided it meets the applicable criteria, and then destroyed or otherwise disposed of in accordance with applicable policy and procedures.
 - b) Mis-shipped Product (Incorrect cannabis product or accessory purchased from BCCS online which was delivered in error to a retail customer.)
 - Shall be accepted for return at any BCCS Store, and;
 - Within one year of BCCS commencing operations, shall be accepted for return by mail, through the Customer Care Centre
 - c) Recalled Product (where a recall has been authorized by BCLDB)
 - Shall be returned in accordance with the provisions of the Product Recall policy.
 - d) Saleable Product (Any cannabis accessory – not product – which has not passed any relevant expiry date, remains in original condition and packaging, and it unopened with all original seals and labels intact)
 - May be accepted for return for refund only, within **15** days of purchase if:
 - Proof of purchase is provided;
 - All layers of the original packaging are unopened with no evidence of tampering, and;
 - A shipping error occurred (for product purchased from BCCS online).
 - Shall be re-stocked in accordance with established BCCS store inventory procedures.
 - May only be returned at a BCCS retail store and not online.



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

Part 1 – General

Name of Ministry:	Ministry of Attorney General, Liquor Distribution Branch		
PIA Drafter:	Tara A. Ralph, Manager, Information, Privacy and Access Services		
Email:	Tara.Ralph@bcldb.com	Phone:	604-252-6213
Program Manager:	Shawn Ling, Chief Technology Officer		
Email:	Shawn.Ling@bcldb.com	Phone:	604-252-8852

1. Description of the Initiative

The Liquor Distribution Branch (LDB) is one of two branches of Government responsible for the wholesale distribution and retail sale of beverage alcohol and non-medical cannabis. It has a workforce of approximately 4600 full- and part-time employees working across 197 BC Liquor Stores, nine BC Cannabis Stores (online and stand-alone), a Head Office, three Wholesale Customer Centres and three Distribution Centres. The LDB is led by a General Manager and CEO who is responsible for administering the *Liquor Distribution Act* and the *Cannabis Distribution Act*, subject to direction from the Minister.

LDB has an Integrated Service Management program which receive and log details of a support/service request ("ticket"), track, escalate and report on these tickets, and coordinate IT change management activities. Each Support Centre team logs and tracks requests and issues within the integrated service management system. The program ensures cross-functional management and escalation of support tickets, standardization of all support/service delivery processes, integration between lines of business where required, and segregation between lines of business where required.

Thus, it optimizes the way LDB delivers services through it's main Support /Customer Care Centres, which are:

1. Information Technology Support Centre (LDB Support Centre)

The LDB Support Centre provides service to:

- a. LDB employees, service providers and vendor support agents ("customers") to facilitate and coordinate requests for technology or system access, technical troubleshooting, information incidents, and IT change management activities.



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

- b. Current and former LDB employees seeking support with payroll-specific inquiries. Integrated service management for payroll allows for cross-functional management and escalation of payroll queries (i.e., from IT Support to LDB Payroll to TES) ensuring an integrated service model to effectively serve the customer.
- c. Members of the public who need to report technical issues with LDB's public-facing websites (i.e., bcliquorstores.com, bccannabisstores.com).
- d. Individuals applying for a Special Event Permit (SEP) who need to report technical issues with the web-based application and/or process for SEP licensing.

2. Wholesale (Liquor) Customer Care (WCC)

The WCC supports wholesale (business-to-business/B2B) customers within the Liquor line of business who may order through LDB's web store (webstore.bcldb.com) or who have questions about WCC services or liquor products. WCC integrated service management does not involve the collection of personal information.

3. Cannabis Customer Care (CCC)

The CCC supports Business to Business (wholesale via e-commerce) and business-to-customer (B2C/retail e-commerce) customers to resolve queries/issues within the Cannabis line of business. These include answering product-related questions, processing returns of product/accessories, effecting product recalls, and resolving customer-reported issues.

The LDB's Integrated Service Management program is planning on using a new integrated, innovative, multi-level IT service management (ITSM) software solution developed by Marval Software, a British company with distributors worldwide. Through a network of 'Authorised Global partners', which are independent companies with local territory knowledge appointed by Marval Software Limited to distribute its products and services, Marval is able to provide ITSM software solutions and support to customers globally.

The authorized partner for Canada is Stroma Service Consulting Inc. ("Stroma"). The ITSM solution is a Software as a Service (SaaS) that will be hosted and maintained by Stroma on a private cloud offering located on Canadian data centres hosted by Strategic Alliance of Business Technology Disciplines ("SABTD"), a Canadian company with no legal ties outside of Canada. In a private cloud, the cloud infrastructure is operated solely for a specific organization and is managed by the organization or a third party. In this case, the cloud infrastructure will be operated solely for Stroma and will be owned and managed by SABTD.



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

Stroma is owned by Logitek Technology Ltd., ("QLogitek"), a subsidiary of Smart Employee Benefits Inc. ("SEB"). Both QLogitek and SEB are Canadian companies with no link to the companies outside of Canada.

Authorized employees of Stroma and SABTD will have access to the personal information located in the LDB's Integrated Service Management system for maintenance, repairing, troubleshooting or upgrading the system.

SABTD will manage the network security of the data centres and security of the servers at the operating system level. SABTD will also be responsible for the secure configuration and patching of the databases; the maintenance and operation (including monitoring and follow-up on malware detected) of the antimalware tool; and the detection and mitigation (i.e., patching and secure configuration) of security vulnerabilities.

Inventory of service system components including a common shared network diagram identifying the network zones is maintained jointly by SABTD and Stroma. LDB's security team will log and monitor changes to its firewalls and routers and will confirm that all changes to the network are reviewed and approved by Stroma and Strategic.

End-users (i.e., LDB and LCRB support staff) will access the system through an Internet connection (i.e., no direct dedicated network connection) and authenticate themselves through local system accounts or via LDB's Identity and Access Management (IAM). Another PIA is currently being completed for IAM and is out of scope of this PIA.

Stroma may, in rare occasions, share personal information with Marval to manage technical issues by way of telephone conversation, email or through cooperative tools such as Webex or Microsoft Teams. Marval will not have direct and ongoing access to the solution and the personal information that will be located in it.

2. Scope of this PIA

This PIA will assess the privacy implications of LDB's Integrated Service Management System.

3. Related Privacy Impact Assessments

SBRT17008 Marval's Integrated IT Service Management Application (MSM)
SBRT17001 Call Centre Anywhere/Telus Cloud Contact Centre (TC3)
AG18064 Cannabis Customer Care
JAG15001 Special Occasion Licence Online (SOLO)



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

4. Elements of Information or Data

The following information may be stored in the application:

- Employee/Customer First Name
- Employee/Customer Last Name
- Employee/Customer Email Address
- Employee/Customer Phone Number
- Customer Shipping Address
- Customer Billing Address
- Business License Number (Wholesale)
- Order Tracking Number (Liquor, Cannabis)
- Description of return (Liquor, Cannabis) including date of purchase, purchase quantity, return quantity
- Details of inquiry/request/return/technical issue:
- LDB Employees payroll/benefits details when they email a service request
- Order details of Cannabis Retail Customers
- Wholesale Liquor Customers (No personal data)
- Cannabis Wholesale Customers (No personal data)

Customer IP addresses will not be collected as tickets will be logged by LDB staff.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information stored on the Integrated Service Management System will be located in Canada on Canadian data centres in Vancouver and Toronto and will only be accessed within Canada. Note that in the context of troubleshooting the public body and its service providers may disclose personal information to Marval UK as per section 33.1(1)(p) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA).



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Personal information is collected as part of LDB daily operations.	Out of scope of this PIA	n/a



Privacy Impact Assessment for LDB Integrated Service Management PIA#AG20047

2.	The personal information is entered on the new Integrated Service Management System located on a Canadian data center.	Use Storage	32(a) and (c) 30.1
3.	The personal information may be temporarily disclosed outside of Canada to Marval UK for technical support and maintenance ONLY with the direct permission of the public body.	Access Disclosure	30.1(b) 33.1(1)(p)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes.	Standards of Conduct Privacy Training	Low	High
2.	Contractors could access personal information and use or disclose it for personal purposes.	Stroma and subcontractors are bound by contract with LDB which includes a Privacy Protection Schedule. Contractor Privacy Training	Low	High
3.	Customer's personal information is compromised when transferred to the service provider.	Transmission is encrypted over the Internet	Low	High

10. Collection Notice

The direct collection of the personal information will be outside of the scope of the PIA. Collection notices will be employed by LDB programs prior to the project data being tracked in the new Integrated Service Management System.

Part 3 – Security of Personal Information

LDB conducted a Security Threat Risk Assessment



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

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

Access to LDB buildings housing support/contact centre staff are only accessible to employees with a key card, or to authorized third parties who have signed in at reception and are accompanied by an employee. LDB laptops are maintained securely by employees and business data cannot be accessed without authentication into LDB's virtual private network.

Other physical security measures of LDB buildings housing support/contact centres include:

- High security locks and keys
- Key cards - each key card is associated with a specific employee and access swipes are logged and auditable
- Internal and external building surveillance
- Security personnel on site 24/7 (warehouses)
- Locked cabinets for shipping lists and un-affixed labels
- After-hours alarm system which notifies security and police in the event the alarm is triggered

s.15; s.21



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

s.15; s.21

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

Integrated Service Management system components consist of a SaaS application, application and database servers (IaaS), databases, and network devices (e.g., firewalls, and routers).

End-users (i.e., LDB and LCRB support staff) will access the system through an Internet connection (i.e., no direct dedicated network connection) and authenticate themselves through local system accounts or via LDB's Identity and Access Management (IAM).

s.15; s.21



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

s.15; s.21

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

The LDB has its own Information Security Policy. It is based on BC Government's Information Security Policy. In turn both of the policies are based on ISO 27001 security standard. Consequently, LDB policy is consistent with Government's but has been adapted for the LDB environment.

14. 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.

End-user access to the integrated service management system is managed by LDB IT Service Management ("account administrators") or IT System Security ("system administrators"). Authentication of users is facilitated via Active Directory to ensure role-based access. User permissions for LCRB staff are managed directly by LDB's System Administrators. Single-factor authentication is in place with complex password required.

Account Administrators: Role-based access is limited to a subset of LDB employees who are tasked with administering user accounts. Tasks and access include: creation of users; deletion of users; modifying existing users; activating requests (i.e., registration) and viewing user lists.

System Administrators: Role-based access is limited to a subset of LDB employees who are tasked with system maintenance, change control, and troubleshooting.

Stroma (i.e., application support) will only connect from a limited number of pre-identified IP addresses will be technically prohibited from accessing the system from outside of Canada. Connection to LDB's instance of the software occurs in response to a service request from LDB.

Access to the data center resources will be controlled by whitelist of remote users to allow only permitted users access.

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

A full auditable request history is maintained within the Integrated Service Management system.



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

All access to resources in the application will be logged by the application and viewable by application administrators for auditing purposes. Each application user will have a login credential, which will be assigned with access permissions necessary for carrying out their duties. When users access personal information that will be stored in the application, the user's credentials and time of access will be logged automatically by the system. Authorized LDB IT Security staff will access audit log information at standard intervals (e.g., via ArcSight for governance, risk and compliance) to detect and/or investigate any abnormalities.

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. 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?**

Customers or employees can contact the support/service centre and request that their personal information be updated (e.g., providing a new phone number or email). If the information is not corrected, an annotation will be made to the file and if the information has been provided to another party in the last 12 months, LDB will advise the party of the request.

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

No, this is only about the new Integrated Service Management System

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

N/a.

- 19. If you answered "yes" to question 17, 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?**

N/a.



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

Part 5 – Further Information

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

There will be systematic sharing of information between the service provider, including subcontractors, and the LDB. However, the service provider is defined as an employee of the LDB as per Schedule 1 of FOIPPA and as such there is no requirement to develop an information sharing agreement.

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

No.

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

Personal Information Bank – Required Information	
Description	Liquor Distribution Branch's details of support/service requests ("ticket").
Primary ministry/government agency involved	Ministry of Attorney General, Liquor Distribution Branch
All other ministries/government agencies and public bodies involved	Ministry of Attorney General, Liquor and Cannabis Regulation Branch
Business contact title	Manager, Information, Privacy and Access Services
Business contact telephone number	604-252-6213



Privacy Impact Assessment for LDB Integrated Service Management

PIA#AG20047

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Jessica Bouchard

July 8, 2020

Privacy Analyst
Privacy, Compliance and
Training Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

Date

Cole Lance

July 13, 2020

Privacy Advisor
Privacy, Compliance and
Training Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

Date



Privacy Impact Assessment for LDB Integrated Service Management PIA#AG20047

Part 7 - Program Area Comments and Signatures

Karine Bordua
Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 14, 2020

Date

Charmaine Lowe
A/Assistant Deputy Minister and
Chief Information Officer
Information Systems Branch
Ministry of Attorney General

Signature

July 27, 2020

Date

Shawn Ling
Chief Technology Officer
Liquor Distribution Branch

Type text here

Signature

October 1, 2020

Date

Peter Kho
Chief Information Security Officer
Liquor Distribution Branch

A/CISO

Signature

October 9, 2020

Date

Nigel Carroll
Chief Information Officer
Liquor Distribution Branch

Signature

October 6, 2020

Date

R. Blain Lawson
General Manager and Chief
Executive Officer
Liquor Distribution Branch

Signature

10/9/2020

Date



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance and the
Administrator of the Cannabis Distribution Act*
PIA#FIN19002

Name of Ministry:	Ministry of Finance (FIN)		
PIA Drafter:	Claire Lovell, Project Officer		
Email:	Claire.Lovell@gov.bc.ca	Phone:	778 698-9665
Program Manager:	Treana Clarke, Manager, Intergovernmental Relations		
Email:	Treana.Clarke@gov.bc.ca	Phone:	778 698-1764

1. Description of the Initiative

The following PIA is being submitted in conjunction with the new information sharing agreement titled – “Agreement for the Exchange of Information (the Agreement) between the Minister of Finance (FIN) and the Administrator of the Cannabis Distribution Act (the Administrator).”

The Government of Canada announced the legalization of non-medical cannabis effective October 17, 2018. Provincially, the Liquor Distribution Branch of the Ministry of the Attorney General (LDB), solely administers the wholesale distribution of all non-medical cannabis for the province of British Columbia (BC). The LDB administers the collection, use and disclosure of information related to the wholesale, distribution and sales of non-medical cannabis in BC.

All cannabis sales in the province of BC are subject to provincial sales tax (PST) under the *Provincial Sales Tax Act* (PST Act) unless the sale is determined to be exempt from PST. FIN requires from the LDB, cannabis sales information for the purpose of administering and enforcing the tax enactments listed in Appendix A of the Agreement. Under the PST Act, LDB is required to ensure that the prescribed requirements to authorize the sale of cannabis exempt from PST, to a Cannabis Licensee, are met at the time of purchase.

Information exchanged will be used for the purpose of administering and enforcing the following taxation enactments:

- *Income Tax Act*, R.S.B.C. 1996, c.215
- *Provincial Sales Tax Act*, S.B.C. 2015, c.35

LDB requires from FIN, PST registrant information for the purposes of confirming a Cannabis Licensee’s authorization to purchase Cannabis exempt of PST. LDB also requires from FIN, PST debtor information relating to debts owed by a Cannabis Licensee for the purpose of assisting FIN in administering the PST Act.

The Agreement does not contemplate the collection, use or disclosure of personal information as defined in FOIPPA. However, while the likelihood of occurrence is very low, it may be possible to piece together cannabis sales information, disclosed by LDB to FIN and then subsequently disclosed to the Canada Revenue Agency (CRA), with CRA information to derive a rough estimate of an individual’s gross income (personal information). This would only occur where a sole proprietor’s only source of income was derived from the sale of cannabis.



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

2. Scope of this PIA

This PIA covers the collection, use and disclosure of cannabis sales information from LDB and FIN's disclosure of PST information to LDB, as detailed in the Agreement.

3. Related Privacy Impact Assessments

There are no related PIAs.

4. Elements of Information or Data

FIN will collect and use the following cannabis sales information from LDB on a monthly basis:

- Purchase Fiscal Period
- Purchase Period Start Date
- Invoice Number
- Cannabis Licence Number
- Cannabis Licensee Name
- Cannabis License Type
- PST Registration Number of Licensee
- Business Number of Licensee
- Invoice Date
- LDB Cannabis Store Number
- LDB Cannabis Store Name
- Total Cannabis Related Purchases (in dollars) (before PST/GST)
- Flower Cannabis Purchases (in dollars and kilogram equivalent)
- Pre-Roll Cannabis Purchases (in dollars and kilogram equivalent)
- Oil Cannabis Purchases (in dollars and milliliters equivalent)
- Seeds Cannabis Purchases (in dollars and selling unit)
- Cannabis Accessories Purchases (in dollars and selling unit)
- Concentrate Purchases (in dollars and selling units)
- Edible Purchases (in dollars and selling units)



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

FIN will collect and use the following cannabis sales information from LDB on an ad hoc basis:

- Purchase Fiscal Period
- Invoice Number
- Cannabis Licence Number
- Invoice Date
- LDB Cannabis Store Number
- Stock Keeping Unit Number
- Product Name
- Quantity Sold
- Selling Unit Measure
- Shipping Unit Measure
- Flower Cannabis Purchases (in dollars)
- Pre-Roll Cannabis Purchases (in dollars)
- Oil Cannabis Purchases (in dollars)
- Seeds Cannabis Purchases (in dollars)
- Cannabis Accessories Purchases (in dollars)
- Concentrate Purchases (in dollars)
- Edible Purchases (in dollars)
- Total Edible Purchases Purchase Amount (in dollars)
- Business Number of Cannabis Licensee
- PST Registration Number of Licensee

FIN will disclose the following PST registrant information to LDB on a quarterly basis:

- Cannabis Licence Number
- Business Number of Cannabis Licensee
- Business Program Identifier and Program Account Number
- PST Registration Number
- Relationship Reason (licence added/licence removed)
- PST Effective Date
- PST Closed Date



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

- Reactivation Date
- PST Registration Number and Cannabis Licence Number Linkage Date
- Cannabis Licence Status (active/cancelled, dormant, expired, inactive, suspended, transferred)
- Cannabis Licence Ownership (licence owner, licence non-owner, unauthorized, related)

FIN will disclose the following PST debtor information to LDB on a monthly basis:

- Legal Entity Name of Debtor
- PST Registration Number
- Cannabis Licence Number
- Cannabis Licence Status
- Cannabis Licence Class
- Cannabis Licence Owner Start Date

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

There is no intention to store or access this information outside of Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	yes
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

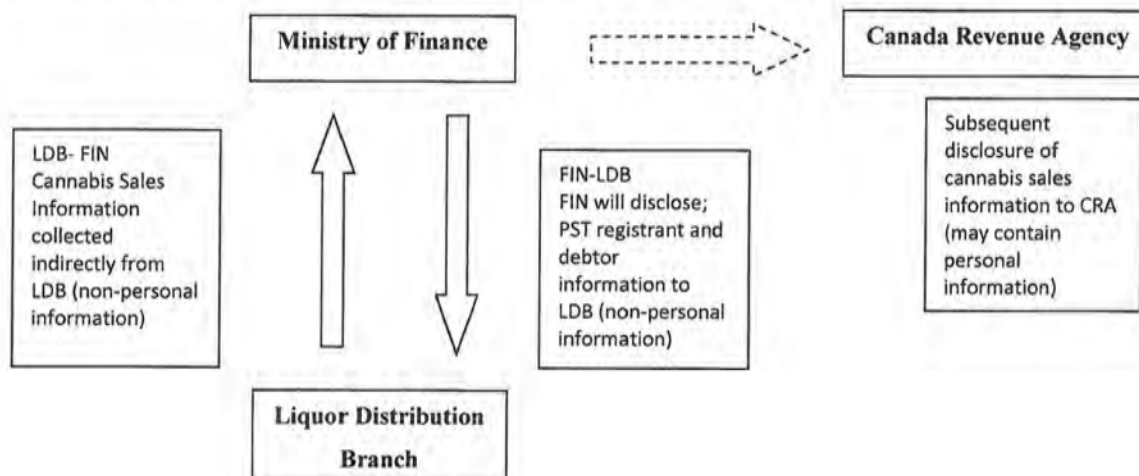
PIA#FIN19002

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

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





Privacy Impact Assessment for the

Exchange of Information Between the Minister of Finance and the Administrator of the Cannabis Distribution Act

PIA#FIN19002

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	The Ministry of Finance (FIN) collects cannabis sales information indirectly from LDB.	Indirect Collection	S.26(a) [Section 195 of the PST Act]; S.27(1)(a)(iii) [Section 195 of the PST Act] & S.27(1)(b) [33.1(1)(c) [Section 195 of the PST Act]]
2.	Information collected from LDB is used to administer and enforce FIN's taxation enactments, primarily the PST Act	Use	S.32(a)
3.	FIN may subsequently disclose cannabis sales information to the Canada Revenue Agency (CRA). The CRA administers and enforces the <i>Income Tax Act</i> , R.S.B.C. 1996, c. 215, on behalf of the province, under the terms and conditions of the Tax Collection Agreement. The Tax Collection Agreement was entered into under section 69 of the <i>Income Tax Act</i> . Information provided to the CRA is done so under the terms and conditions of the <i>Memorandum of Understanding Establishing an Administrative Framework for the General Provision of Information and the Promotion of Cooperation and Mutual Assistance between the Canada Revenue Agency and the British Columbia Ministry of Finance</i> , an agreement entered into under the authority of paragraph 65(2)(a) of the <i>Income Tax Act</i> (British Columbia).	Disclosure	S.33.2(a); S.33.1(1)(d) [Section 228(1)(d) of the PST Act]
	FIN will disclose PST registrant and debtor information to LDB to administer and enforce FIN's taxation enactments, primarily the PST Act.	Disclosure	S.33.1(1)(c)[Section 228(1)(a) of the PST Act]



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	FIN employees could derive personal information and use or disclose it for personal purposes	Annual Oath of Employment Province wide mandatory privacy training Annual Standards of Conduct	Low	High
2.	Information is compromised at the time of exchange, for example, when receiving it from LDB or when providing it to the CRA	Transmission is encrypted and over a secure line	Low	High

10. Collection Notice

Given that the information is being collected indirectly from LDB, there is no collection notice as one is not required per section 27(3)(c) of FOIPPA. The indirect collection is authorized per Section 27(1)(a)(iii) and Section 27(1)(b).

Part 3 – Security of Personal Information

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

Entry into the FIN buildings and to each floor where the computer terminals are located requires a key card. Information is stored in a secure database and is accessed through password-protected computers.

For employees working outside the workplace, they must conduct their work in a secured and approved workplace with reasonable security measures to safeguard storage devices; including but not limited to reducing visibility and keeping control of the device or information.

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

FIN users must be approved for role-based access, set-up with a profile and assigned a password to connect to applications on a need-to-know basis. As well, external access to the information is restricted by government firewalls. Those FIN users that telework access the Government network through an approved secure connection. Laptop computers have encrypted hard drives and the ability for remote desktop connection with Virtual Private Network.



Privacy Impact Assessment for the

Exchange of Information Between the Minister of Finance and the Administrator of the Cannabis Distribution Act

PIA#FIN19002

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

Given FIN's close working relationship with the CRA and the amount of information exchanged between the two parties, FIN also relies on the CRA's Security Standards for the Protection of Client Information. This set of standards created by the CRA is an extensive list of minimum policies and procedures to ensure that information is only accessed and used on a need-to-know basis.

Information that is subsequently shared with the CRA, through this initiative, is done so in accordance with the CRA's security protocols.

14. 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?

All of the applications used by FIN require the use of user IDs and passwords before access is granted. Transaction records are stamped with users' names and dates so that log files can be reviewed or so that user IDs can be displayed within an application's interface. All of FIN's applications also have role-based security to limit access to functions that are required to perform a particular employee's duties only. FIN also implements controls designed to ensure that adequate and proper separation of duties exist in order to ensure that posted transactions are authorized. These controls require that transactions must go through multiple levels of approvals.

In the context of this initiative, the information provided by LDB is not changed by FIN. It is used to corroborate with information provided by the taxpayer to confirm compliance with tax liabilities established under the laws listed in the Agreement.

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

The LDB file is uploaded into the data warehouse of FIN systems. Where a file is electronically stored in FIN application, user access groups are reviewed semi-annually, at minimum. This review is conducted to ensure that only authorized staff are members of groups that have access to information. A log of action also records staff accesses to data in the system. User activity logs are reviewed on a monthly basis.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. 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?

The information provided by LDB is not changed. It is used to corroborate with information provided by the taxpayer to confirm compliance with tax liabilities established under the laws listed in the Agreement.

A taxpayer has the opportunity to provide information to FIN during an audit, which is taken into consideration by FIN when determining tax compliance. FIN has the ability to annotate records by inserting notes into a file.



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

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

While none of the information exchanged in the initiative is personal information, it may be used to audit sole proprietors. During an audit, the taxpayer has the opportunity to confirm compliance with the tax obligations by providing financial books/records. Information provided by LDB is used to corroborate with information provided by the taxpayer. An audit may lead to the issuance of a Notice of Assessment or Notice of Reassessment to the taxpayer.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

If a taxpayer believes the Notice of Assessment/ Reassessment is based on inaccurate or incomplete information, the taxpayer has the right to appeal any decision by FIN. This appeal process also provides the individual with the opportunity to ensure information in FIN's custody is accurate and complete.

19. If you answered "yes" to question 17, 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?

Yes. FIN adheres to an approved records retention and disposition schedule in line with the Government of British Columbia's policies concerning retention and disposition of records.

Part 5 – Further Information

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

Yes. While the initiative does not contemplate the disclosure of personal information, there is a systematic disclosure of information and it is FIN's practice to enter into an Information Sharing Arrangement, regardless of whether true personal information is involved.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.

✓



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

Information Sharing Agreement – Required Information	
Description	Agreement for the Exchange of Information (the Agreement) Between the Minister of Finance (FIN) and the Administrator of the Cannabis Distribution Act (the Administrator)
Primary ministry/government agency involved	Ministry of Finance
All other ministries/government agencies and public bodies involved	The Liquor Distribution Branch
Business contact title	Manager, Intergovernmental Relations, Treana Clarke
Business contact telephone number	778.698.1764
Indication of whether or not personal information is involved	No
Start date	October 17, 2018
End date (if applicable)	Indefinitely

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

No.

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

No. Information collected from LDB is stored in existing PIBs.

Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act
PIA#FIN19002*

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry

Privacy Analyst
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

January 16, 2019

Date

Quinn Fletcher

Director, Operations and Privacy
Management
Privacy, Compliance and Training
Branch
Corporate Information and
Records Management Office
Ministry of Citizens' Services

Signature

January 23, 2019

Date



Privacy Impact Assessment for the

Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act

PIA#FIN19002

Part 7 – Program Area Comments and Signatures

Jeffrey Krasnick

Director, Income Tax Advisory and
Intergovernmental Relations
Income Taxation Branch
Ministry of Finance

Signature

Date

Feb 15/19

Richard Barlow

Ministry Privacy and Information
Security Officer
Information Management Branch
Ministry of Finance

Signature

January 24 2019

Date

for Kevin Harris or
Michelle Lee

Executive Director
Consumer Taxation Programs
Branch
Ministry of Finance

Signature

Date

Feb 19/19

Francis Camilleri

A/ Executive Director
Income Taxation Branch
Ministry of Finance

Signature

Date

February 19, 2019

Jordan Goss

Assistant Deputy Minister
Revenue Division
Ministry of Finance

Signature

Date

Feb 22, 2019

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.



Privacy Impact Assessment for the

*Exchange of Information Between the Minister of Finance
and the Administrator of the Cannabis Distribution Act*

PIA#FIN19002

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. If you have any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.