VSA
VEHICLE SALES AUTHORITY OF BC

MOTOR VEHICLE SALES AUTHORITY

PRIVACY POLICIES AND PROCEDURES

Effective May 20, 2024
Ver. 2

Table of Contents

Record of Updates

Version	Date	Summary of Update
1	November 1, 2014	Original
2	May 20, 2024	Added: Policy Statement Record of Update Breach Reporting Protocol New VSA Logo References to amended legislation Standardized Terms for Vendor Contracts Expanded PIA Policy and Review Website policy statement language

1. Introduction

1.1. Policy Statement

The Vehicle Sales Authority of British Columbia ("VSA") is committed to protecting the personal information we collect, use, disclose, and store from members of the public and from staff. This includes information pertaining to licensees, consumers, employees, and other stakeholders. When we collect personal data, we are taking on the responsibility of safeguarding the integrity of the data and being accountable for its life cycle. We have a privacy management program (PMP) to ensure that we abide by applicable laws while fulfilling our legislative mandate.

To safeguard personal information, the VSA commits to complying with the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Motor Dealer Act*, provisions of the *Business Practices and Consumer Protection Act* and other applicable legislation. This covers both personal information collected from external stakeholders and collected from employees and staff members within the VSA.

1.2. Purpose of the Policies and Procedures

The VSA is a listed public body subject to the *Freedom of Information and Protection of Privacy Act* of British Columbia. In carrying out its administration of the *Motor Dealer Act* (the "MDA") and portions of the *Business Practices and Consumer Protection Act* (the "BPCPA") in the public interest, the VSA is granted statutory authority to compel production of personal, financial, commercial, proprietary or otherwise confidential information.

The purpose of these policies and procedures are to:

1. Ensure compliance with the *Freedom of Information and Protection of Privacy Act* and the confidentiality provisions of the *Motor Dealer Act*.
2. Provide guidance to staff and vendors regarding their obligations in collecting, using, disclosing and securing confidential information.
3. Promote transparency in the operations of the VSA.
4. Consolidate various past policies and procedures related to privacy into one document.

For any policy or procedure not identified in these policies and procedures, the VSA will use the FOIPPA Policy and Procedures Manual of the Office of the Chief Information Officer for British Columbia to be modified as necessary for VSA operations: http://www.cio.gov.bc.ca/cio/priv_leg/foippa/guides_forms/guide_index.page,.
This document is intended to align with the OIPC's privacy management program, in the document entitled "Accountable Privacy Management in BC's Public Sector":

https://www.oipc.bc.ca/guidance-documents/1545.

1.3. Important terms

Some important terms and acronyms that will be used throughout these policies:

Administrative Agreement	means the Administrative Agreement dated for reference March 24, 20(between Her Majesty the Queen in right of British Columbia Crown (Government) and the Motor Dealer Council of British Columbia
BPCPA	means the *Business Practices and Consumer Protection Act,* SBC 2004 2.
Board Appointee	means a person appointed to the Board of Directors of the VSA but has as yet attended their first meeting.
Commissioner	means the Information and Privacy Commissioner of British Columbia
.Confidential Information	means information collected by the VSA where there is a reasonable expectation that it will be kept confidential and includes personal information, proprietary information, financial information, or any othe information that is protected from disclosure by law.
Contact information	has the same meaning as in Schedule 1 of FIPPA.
FIPPA	means the *Freedom of Information and Protection of Privacy Act,* RSB 1996, c 165.
FIPPA-R	the *Freedom of Information and Protection of Privacy Act Regulation,* I Reg 155/2012.
License, licensed, and licensing	means a registered motor dealer, a licensed salesperson, a licensed wholesaler, a licensed broker-agent, a licensed broker-agent representative, and a wholesaler representative as those terms are defin in the MDA
MDA	Means the *Motor Dealer Act,* RSBC 1996, c 316.
MDCCFB	means the Motor Dealer Customer Compensation Fund Board as define in the MDA.
MDCCFB Member	means a person who has been appointed to the MDCCFB.
OIPC	means Office of the Information and Privacy Commissioner of British

	Columbia.
Personal information	has the same meaning as in Schedule 1 of FIPP.
PIA	means a Privacy Impact Assessment.
Privacy Officer	means the person who has been delegated, pursuant to section 66 of FIPPA, the authority of the Head of the VSA and or the Head of the MDCCFB to ensure compliance with FIPPA.

1.4. VSA's Mandate & Legislative Authority

The VSA was created to administer the MDA and portions of the BPCPA in relation to consumer sales of motor vehicles within the motor dealer industry. The core functions of the VSA are:

1. Licensing of motor dealers and salespersons which includes background checks.
2. Inspection of motor dealers and salespersons for compliance with the MDA and the BPCPA.
3. Investigation of complaints against motor dealers and salespersons.
4. Informal dispute resolution of complaints made against motor dealers and salespersons where appropriate.
5. Conducting quasi-judicial licensing and consumer complaint hearings and prosecution of offences under the MDA and/or the BPCPA.
6. Processing and adjudicating claims against the Motor Dealer Customer Compensation Fund.
7. Education of the industry and the general public regarding the motor vehicle sales marketplace.
8. Advice to the British Columbia government on any aspect of the motor vehicle sales marketplace.

The VSA obtains its legislative authority to compel disclosure of information and records from the MDA, the BPCPA, and their regulations, and ancillary authority under provisions of the *Interpretation Act,* RSBC 1996, c 238.

1.5. General Principles to be Applied to Personal Information

To safeguard privacy, the VSA shall treat personal information according to these principles:

- Personal information is to be disclosed to staff and other stakeholders on a pure "need-to-know" basis;
- Personal information is to be used, disclosed, and stored only if doing so is consistent with the original purpose for which the personal information was collected;
- Except as authorized by legislation, any secondary use of personal information – that is, any use of personal information that differs substantively from the original purpose for its collection – requires express written consent from the person(s) to whom the personal information pertains;

- The VSA does not and will not sell any information, including personal information to third parties; and
- Internal access to any personal information is assigned based on the role of the staff member and their need to access the personal information.

The principle of "least privilege" governs. This means that only the minimum amount of personal information required to perform a task shall be granted at all times.

1.6. Applicability of these Policies and Procedures

This Privacy Policy applies to all personal information or personal identification information collected by the VSA from consumers, licensees, employees, and other stakeholders. Additionally, these privacy protection requirements apply to all VSA staff, including employees and service providers. It is therefore incumbent upon the entire organization to safeguard personal information in the VSA's custody.

1.7. For more information

Any person who has questions or needs more information about the VSA's Privacy Policy should contact the VSA:

- by e-mail at privacy@mvsabc.com
- by phone at 604-574-5050
- by fax at 604-574-5886
- by mail at Suite 280 – 8029 -199 Street, Langley, BC V2Y OE2

2. Training

2.1. New Staff, Board Appointee, or MDCCFB Member

New staff members, Board Appointees and MDCCFB Members must attend a privacy training session with the Privacy Officer as part of their orientation. This training should occur before they have access to *confidential information*. The training session will cover:

1. Overview of the FIPPA.
2. The five major components of FIPPA.
3. Sources of information at the VSA.
4. The *Personal Information Protection Act* (PIPA).
5. The relationship between FIPPA, PIPA and the MDA.
6. Collection, use, disclosure and security of information held by the VSA

7. Privacy breach protocols
8. Other key procedures to follow, and
9. Employee obligations under FIPPA and the MDA.

2.2. Ongoing training

The Privacy Officer will conduct a refresher course at least once per year for all staff members. Additional training will be identified and provided as needed.

3. Heads of the Organizations

3.1. Head of the VSA

3.1.1. The Head of the VSA is responsible for ensuring compliance with FIPPA and responding to any access requests made under FIPPA.

3.1.2. The Head of the VSA is the Chair of the VSA Board of Directors. [Schedule 2 of FIPPA]

3.2. Head of the Motor Dealer Customer Compensation Fund Board

3.2.1. The Head of the MDCCFB is responsible for ensuring compliance with FIPPA and responding to any access requests made under FIPPA.

3.2.2. The Head of the MDCCFB is the Chair of the VSA Board of Directors. [Schedule 2 of FIPPA]

3.3. Privacy Officer

3.3.1. The Head of the VSA and the Head of the MDCCFB may delegate their duties and obligations under FIPPA to any person. [s. 66 - FIPPA]

3.3.2. The Head of the VSA and the Head of the MDCCFB may at any time alter or rescind their delegation noted in paragraph 3.3.1. [s. 66 - FIPPA]

3.3.3. The Head of the VSA and the Head of the MDCCFB have delegated their duties and obligations under FIPPA to the Privacy Officer. [s. 66 - FIPPA]

4. Collection of Information

4.1. Collection is necessary

4.1.1. The VSA should collect only the personal and confidential information that is necessary to carry out its mandate. [s. 26 - FIPPA]

4.1.2. The types of personal and confidential information that the VSA collects, the categories of persons it is collected from, and the authority to collect are set out in **Appendix A.** [section 69(6) - FIPPA]

4.2. Direct collection

4.2.1. Whenever possible, the collection of personal and confidential information should be directly from the person the information relates to and with their consent. [s.26 - FIPPA]

4.3. Indirect collection

4.3.1. Indirect collection of personal or confidential information (i.e. without the person's consent or knowledge) may occur where direct collection will interfere with the VSA carrying out its mandate, such as interfere with an investigation and the indirect collection is:

(a) Authorized by the MDA, the BPCPA or FIPPA [s. 27(1)(b) - FIPPA]
(b) For a proceeding before a court or a hearing before the Registrar [s. 27(1)(c)(ii) - FIPPA]
(c) For collecting a debt owed to the VSA or the MDCCFB [s. 27(1)(c)(iii) - FIPPA]
(d) For law enforcement purposes which includes investigations under the MDA [s. 27(1)(c)(iv) - FIPPA]
(e) Under another enactment of law in Canada [s.27(c.2) – FIPPA]
(f) Necessary to manage or decide to terminate an employee of the VSA [s. 27(1)(c.2) - FIPPA]
(g) Confidential information transferred by another public body to the VSA so the VSA may respond to an access request under FIPPA [s.27(1)(d) - FIPPA]

There are other exceptions which generally do not apply to VSA operations.

4.4. VSA to provide information upon collection

4.4.1. Where personal information is collected, including from an employee of the VSA, the VSA must:

(a) Advise the person the purpose of its collection,
(b) The legal authority to collect the information, and
(c) The title and contact information of a person at the VSA who can answer questions about the collection of personal information.[s. 27(2) – FIPPA]

4.5. When the VSA need not provide information upon collection

4.5.1. The VSA need not provide the information required in 4.4.1, where:

(a) The information is about law enforcement or anything which may harm a law enforcement matter, including procedures used to conduct investigations [s. 27(3)(a) - FIPPA]
(b) The VSA is excused from providing notice by the Minister [s. 27(3)(b) - FIPPA]
(c) The VSA is authorized to collect the information indirectly [s. 27(3)(c) - FIPPA]
(d) The information is collected by observation at an event open to the public and where the person the subject of the information voluntarily appears (ex. a concert, ceremony, or sports event) [s. 27(3)(d) - FIPPA]

4.6 Accuracy of information collected

4.6.1. The VSA must take reasonable steps to ensure the accuracy of personal information it collects from an individual and where it will retain and use that information to make a decision directly affecting the individual. [s. 28 - FIPPA]

4.7 Procedures for collecting information

4.7.1 The procedures to be followed when collecting information for VSA purposes are documented in each of the policy and procedure manuals for individual VSA departments including:

(a) Consumer Services Policy and Procedures,
(b) Investigations Policy and Procedures,
(c) Industry Standards Policy and Procedures,
(d) Licensing Policy and Procedures,
(e) Hearing Policy and Procedures Manual, and
(f) Motor Dealer Customer Compensation Fund Board Claim Processing and Adjudication Policy and Procedures Manuals.

4.7.2 The above policies are to be available to the public on the VSA website [ss. 70 & 71 – FIPPA].

5. Use of Information

5.1. Used for the purpose it was requested by the VSA

5.1.1. The VSA may use personal and confidential information in its custody or control for the purpose for which it was collected [s. 32(a) - FIPPA].

5.1.2. The various uses of personal and confidential information the VSA collects has been identified in **Appendix A.**

5.2. Used for a consistent purpose

5.2.1. The VSA may use personal and confidential information in its custody or control for a purpose that is consistent with the original purpose for which it was collected [s. 32(a) – FIPPA].

5.2.2. For paragraph 5.2.1, a purpose is consistent with the original purpose where:

(a) It has a reasonable and direct connection to the original purpose, and
(b) The use is necessary for the VSA to perform its statutory duties, or to carry out an operating program or activity [s. 34 – FIPPA].

5.3. Used for a purpose identified in FIPPA

5.3.1 Collected personal information may also be used for purposes for which the information can be disclosed by a public body under FIPPA [s. 32(c) – FIPPA].

6. Disclosure of Information

Disclosure of information can occur:

(a) As a result of a request for access to information [s. 5 – FIPPA]
(b) As part of the VSA's proactive disclosure of records [ss. 70 & 71 – FIPPA]
(c) As required to safeguard the health or safety of the public [s. 25 – FIPPA]
(d) If it is clearly in the public interest to disclose the information [s. 25 – FIPPA]
(e) Where otherwise authorized by FIPPA [s.33 – FIPPA].

6.1. How a request must be made

6.1.1. A person may request access to information held by the VSA.[s.5 – FIPPA]

6.1.2. A request under paragraph 6.1.1 must be in writing and

(a) Provide sufficient detail to allow the VSA to identify the records using reasonable efforts
(b) Provide written proof of the applicant's authority to make the request, if they are making the request on behalf of someone else, and
(c) Reasonably believes the VSA has custody or control of the record.

[s. 5 – FIPPA]

6.1.3 The VSA encourages the use of the written request form found in **Appendix B**, but must accept any form of written request so long as it complies with paragraph 6.1.2

6.1.4. If the requesting person has difficulty in making a written request because of their unfamiliarity with the English language or a disability impairs their ability to make a written request, then they may make an oral request and the VSA must assist that person to make the request. [s. 6 – FIPPA; s. 2 – FIPPA-R]

6.2. Who may make a request

6.2.1. Any person within or outside Canada may make a request for access to information held by the VSA.

6.2.2. A person may make a request through a representative or agent where:

(a) The requesting person is a minor and is incapable of making the request, then the request may be made by a guardian of the minor, which includes a parent (whether by birth or adoption), a court appointed guardian or the Public Guardian or Trustee acting under the *Public Guardian and Trustee Act* [s. 3 – FIPPA-R].

(b) The request relates to a deceased adult, then the request may be made by:
(i) A Committee acting under the *Patients Property Act*
(ii) If there is no Committee, then the personal representative identified in the will of the deceased
(iii) If there is no Committee or personal representative, then the nearest relative as determined under paragraph 6.2.3
[s. 5(1)(a) – FIPPA-R]

(c) The request relates to a deceased minor, the request may be made by

(i) The personal representative of the minor
(ii) If there is no personal representative, then a guardian of the minor before the date of death,

(iii) If (i) or (ii) do not apply, then the nearest relative as determined under paragraph 6.2.3.

[s. 5(1)(b) – FIPPA-R]

(d) The request relates to an adult under a disability, then the request may be made by a:

(i) Committee under the *Patients Property Act*
(ii) person acting under a power of attorney
(iii) litigation guardian
(iv) representative acting under a representation agreement as defined in the *Representation Agreement Act*

[s. 4 – FIPPA-R]

(e) The requesting party is acting through an agent, including a lawyer, and has provided a written authorization to release specified information, including personal information, to that agent or lawyer. An Authorization for Release of Personal Information and Records Form can be found in **Appendix C** [s. 33(2)(c) – FIPPA].

6.2.3 For paragraphs 6.2.2 (b)(iii) and (c)(iii), the nearest relative is determined as the first person in the following list willing and able to act for the deceased adult or minor:

(a) spouse [either married or living together in a marriage-like relationship for one year] of the deceased at the time of death,
(b) adult child of the deceased,
(c) parent of the deceased,
(d) adult sibling of the deceased,
(e) other adult relation of the deceased other than by marriage, or
(f) an adult immediately related to the deceased by marriage.

[s.5(1) – FIPPA-R]

6.2.4 Where a request for information is from a foreign (outside of Canada) law enforcement agency, court, or state agency, immediately advise the privacy officer who must determine if the request can be fulfilled under an existing written arrangement, agreement or treaty under provincial or Canadian legislative authority [s. 33(6)(b) – FIPPA].

6.3. Forwarding a Request to the Privacy Officer

6.3.1. VSA staff must forward a request to the privacy officer as soon as possible. It is incumbent on the privacy officer to ensure coverage while they are on vacation or if they are on other VSA-associated business and are unable to respond to the request.

6.3.2 The Privacy Officer will engage the assistance of the Legal Administrative Assistant or other VSA staff members as necessary.

6.3.3 VSA staff must not provide the requesting person any information as to when a response to the request will be made or what information will be provided. The privacy officer will contact the requesting person after an application is received.

6.4. Initial Review of a Request

6.4.1. The privacy officer must review the request for compliance with FIPPA, if the request does not meet the requirements, the privacy officer must correspond with the requesting party, identify any deficiency and seek clarification as soon as possible [s. 5 – FIPPA].

6.4.2 The privacy officer ensures a case file with a unique case file number is created in the VSA database where communications will be tracked.

6.4.3 Once the privacy officer confirms that the request meets the requirements of FIPPA, he or she will correspond with the requesting party, acknowledging that the request has been received and noting:

(a) the date the request was received;
(b) the VSA case file number;
(c) that the VSA has 30 business days to respond to the request and provide the date;
(d) that the 30 business days may be extended in certain circumstances and a letter may be sent advising the requesting person for a deposit before any further work is done on the request;
(e) if the applicant would accept electronic disclosure; and
(f) who the requesting person may contact regarding their access request.

6.4.4 All correspondence should be in writing and a copy of all correspondence and notes are to be placed in the electronic case file.

6.4.5. For certainty, "days" within FIPPA has the same meaning as in the *Interpretation Act,* which defines "days" as business and not calendar days.

6.5. Time to Respond to Request

6.5.1. The VSA must respond to an access request no later than 30 business days from receipt unless an extension of time (another 30 business days) is necessary. The VSA must clearly

state the reason for the extension of time and provide an estimated completion date [s. 7 – FIPPA].

6.5.2 If a requesting person has sent the request to the wrong public body, then the following should occur within 20 business days of receiving the access request:

(a) determine the appropriate public body who should process the request;
(b) transfer the request by providing the public body a written letter and enclose the requesting applicant's request; and
(c) notify the applicant in writing that their request has been transferred to the other public body.
[s. 11 – FIPPA]

6.6. Search for Information

6.6.1. The privacy officer must review the request and devise a records search that will locate records responsive to the request. The privacy officer must ensure records in all forms are searched for, including in electronic and hard copy forms.

6.6.2 The privacy officer must ask staff members involved with a file if they have any additional notes that were not placed in the file.

6.6.3 Special attention should be made to requests for investigator's files as investigators may have information in satellite offices or remote workplaces and these must be requested and returned to the main office for review.

6.6.4 Special attention should be made where the request may require disclosure of Crown Records held by the Ministry. The VSA is also responsible for these disclosures.

6.6.5 Special attention should be made where the request may require disclosure of records that were provided to the VSA under an Information Sharing Agreement ("ISA"). Where this is the case, the privacy officer should refer to the ISA to ensure that the records in question may be disclosed and whether the ISA provides any guidelines for such disclosure.

6.7. Providing Fee Estimates

6.7.1. The VSA may charge a fee in certain circumstances that are set out in FIPPA and its regulation (and see the decision of the Privacy Commissioner in *Re*: *Inquiry Regarding British Columbia Securities Commission Records* Order 00-19). A review of various decisions of the Privacy Commissioner indicates clarity as to the service rendered and

accompanying fee is essential.

6.7.2 A fee estimate is to be provided as soon as is possible, and should be provided no later than 20 business days after receipt of the request, unless circumstances require more time.

6.7.3 Fees cannot be charged for:

(a) the first 3 hours spent locating and retrieving a record;
(b) time spent severing a record; and
(c) processing a request for the requesting person's own personal information.

6.7.4 A business may request access to records to carry out their business operations. They can be charged for the actual cost to the VSA for processing their request [s. 75 – FIPPA; Schedule I, Item 2 – FIPPA-R].

6.8. Request to Waive or Reduce Fees

6.8.1 A requesting party may ask that fees be waived or reduced. The following should be considered when deciding to waive or reduce a fee:

(a) The public interest that the information be disclosed;
(b) The nature of the information sought such as:

(i) It contains mostly personal information of the applicant;
(ii) It is information requested by a complainant from an investigation; or
(iii) It is information sought by the media or a party with no direct interest in a file,

(c) The amount of the fee; and
(d) The VSA is a not-for-profit society with no government funding.

***Note**: Where a lawyer is requesting information on behalf of a client, it may be for the purpose of conducting civil litigation. If that is the case, the requesting party may be able to recover fees at trial.

6.9. Redactions/Refusing Disclosure

6.9.1 The purpose of FIPPA is to disclose information with refusal being the exception. The onus is on the VSA to justify a non-disclosure decision [s. 57 – FIPPA].

6.9.2 Where FIPPA grants the VSA discretion to disclose information, the discretion must be

exercised with the following in mind

(a) The purpose of FIPPA
(b) Balance of interests (what is the purpose of the exception)
(c) Ability to sever confidential or protected information
(d) Historical practice
(e) Nature of the record
(f) Will disclosure increase public confidence
(g) Age of the record
(h) Compelling need for disclosure
(i) Previous decisions of the Commissioner, and
(j) The confidentiality provision of section 29 of the MDA.

6.9.3 Refer to FIPPA for guidelines on disclosure. Also, refer to the Information Sharing Agreement and Memorandum of Understanding with I.C.B.C., the Ministry of Finance, Consumer Protection BC, Ontario Motor Vehicle Industry Council, and Financial and Consumer Affairs Authority of Saskatchewan if their information is potentially to be disclosed [s. 12 – 22, 25, and 33 – FIPPA].

6.9.4 The VSA has a legal obligation to protect the identity of confidential sources of law enforcement information – informants.

[s. 15(1)(d) – FIPPA and the common law]

6.9.5 Where an entire document or page of a document is to be withheld, the privacy officer must describe the type of information withheld and the legal authority to do so.

6.9.6 Where a document is to be disclosed, but portions of the page are to be redacted, redact those portions not to be disclosed and include the section number of the Act or its regulation which authorizes its non-disclosure, and a description of the redacted information.

6.9.7 The original electronic copy file is to be copied and left unmarked and unaltered.

6.10. Response to the Request and Disclosure

6.10.1. The privacy officer prepares the records for disclosure and records the number of pages within the records.

6.10.2. Once the review of records is complete and the request is ready for the applicant to receive, a letter is to be sent to the applicant indicating:

(a) If they are entitled to the records;
(b) When and how access will be given;
(c) If a record or part of a record is refused from being disclosed, the VSA must note:

(i) The reason for refusal and the provision of FIPPA allowing its refusal;
(ii) The name and contact information of someone the requesting person can contact to ask questions; and
(iii) That the requesting person can apply to the Privacy Commissioner for a review under section 53 or 63 of FIPPA. The contact information for the Privacy Commissioner's office should be included in the written response.

(d) Despite the above, the VSA may refuse to confirm or deny the existence of a record in a response if:

(i) It is a record containing information covered by a law enforcement matter [s. 15 – FIPPA]; or
(ii) It is a record containing personal information of a third party the disclosure of which would be an unreasonable invasion of that party's personal privacy [s. 23(3) – FIPPA].

[s. 8 – FIPPA]

6.10.3. If the applicant has asked for a copy of the records, they are to be provided a copy of the records (subject to paying any fee). If the applicant has asked to review the records, they may review the records at the VSA office during normal business hours. If the applicant has asked for an electronic copy and it can be easily provided, then the applicant is to receive the records by electronic means [s. 8 and 9 – FIPPA].

6.11. Information that will be published or released within 60 days

6.11.1. The VSA may refuse to disclose to a requesting person information that:

(a) Within 60 business days after the applicant's request is received, it is to be published or released to the public; or
(b) Must be published or released to the public under an enactment.

6.11.2. The privacy officer must notify the requesting person of the publication or release of information that the VSA has refused to disclose.

6.11.3. If the information referred to in 6.1.1 is not published or released to the public within 60

days after the requesting person's request is received, the privacy officer must disclose the information to the applicant within 30 business days, unless disclosure is prohibited under FIPPA [s. 20 – FIPPA].

7. Proactive Disclosure of Information

7.1. Policy Manuals Available Without Request

7.1.1. The VSA must make available to the public, without a formal request under FIPPA, records of the following:

(a) Manuals, instructions, or guidelines issued to the officers or staff of the VSA; and
(b) Rules, or policy statements used by the VSA for interpreting an enactment or administering a program which affects the general public or a specific group.

[ss. 33.3(1) and 70 – FIPPA]

7.1.2. Within the records noted in section 7.1.1., and before making the records available, the VSA may delete any information that it would be entitled to refuse to disclose to an applicant. If information is deleted, the record must include a statement that information has been deleted, the nature of the deleted information and the reason for deletion [s. 70(2) and (3) – FIPPA].

7.2. Records Available Without Request

7.2.1. The VSA may designate categories of records appropriate for routine release to the public [s. 71 – FIPPA].

7.2.2. The categories of records currently identified for routine release are:

(a) Operational Policy Manuals (Licensing, Industry Standards, Investigations, Consumer Services)
(b) VSA's Regulatory Philosophy & Enforcement Principles
(c) VSA's Compliance Enforcement Model
(d) Registrar hearing decisions
(e) Motor Dealer Customer Compensation Fund Board decisions
(f) Undertakings by licensees
(g) The licensing information of motor dealers and salespersons including
    (i) Effective and end dates of licenses
    (ii) Any conditions on licenses
    (iii) Contact information of licensees

(h) VSA Corporate documents including
    (i) Annual reports
    (ii) Financial statements
    (iii) Strategic and business plans
    (iv) The Administrative Agreement between the Crown and the Authority
    (v) The Board of Directors
(i) Information on unlicensed activity
(j) Educational material for consumers and industry members
(k) Industry Bulletins & Dealer Alerts,
(l) Application materials,
(m) Fee schedules, and
(n) Surveys and studies.

8. Request for Correction of Information

8.1. Accuracy of Personal Information

8.1.1. The VSA must make every reasonable effort to ensure that the personal information collected or causes to be collected is accurate and complete [s. 28 – FIPPA].

8.1.2. The VSA must fully document and keep current processes (see 4.7.1) it uses, or that are used on behalf of the VSA to make a decision affecting an individual [s. 28 – FIPPA].

8.2. Right to Request Correction of Personal Information

8.2.1. Applicants have the right to ask the VSA to correct their personal information where it is wrong or to provide additional information where it is incomplete [s. 29 – FIPPA].

8.2.2. The VSA may refuse or be unable to make the correction the applicant requests, either because the applicant has not submitted adequate proof in support of the requested correction or because the information exists in a form that cannot be corrected.

8.2.3 A person may not request correction of factual information that has been found in a formal decision of the Registrar or the Motor Dealer Customer Compensation Fund Board after an adjudication. The person must appeal or request a review of those factual findings to the legal body empowered to review such decisions.

8.2.4 Factual information can be corrected but an opinion, which is a subjective assessment or evaluation of a person's abilities, performance, or other characteristics, cannot.

8.3. Process for Correction of Personal Information

8.3.1. Upon receipt of a written request for correction of a record, the VSA shall correct factual errors when requested to do so by the applicant the information is about if it is supported by adequate proof. Occasionally, this correction can be made by physically changing the original record. This type of change will only be made where the VSA has not used or disclosed incorrect information. The VSA will correct the record by clearly marking the original information as incorrect and attaching the correct information to the record.

8.3.2. The VSA will rectify any omission of information, provided the request is supported by adequate proof, by adding information so that the record is complete.

8.3.3. The VSA may annotate a record by physically adding explanatory notes to it, such as a letter, report, or other document. Alternatively, the applicant could submit an annotated copy of the disputed record for attachment to the original document. [s.29(2) – FIPPA]

8.3.4. The VSA will inform any other public body or organization with which the information was disclosed during the one year period before the correction was requested, of any such correction or annotation, or as required by an Information Sharing Agreement, whichever provides the greater notice.

8.3.5. The VSA will inform the applicant, in writing, that:

(a) The information has been corrected;
(b) The information has been annotated; or
(c) Why a correction is inappropriate or why the proof provided is insufficient or inadequate to make a correction.

8.3.6. The VSA will set up the record or file so that the correction or annotation will always be retrieved with the original record [section 29 – FIPPA].

9. Retention/Security of Information

9.1. Protection of Personal Information

9.1.1. The VSA is to provide appropriate physical, technological, and procedural security measures to protect personal information in its custody or under its control [s. 30 – FIPPA].

9.1.2. The VSA must:

(a) Ensure employees are trained to follow proper security procedures,
(b) Monitor employees' compliance with security standards,
(c) Ensure physical, technological, and procedural security precautions are established and maintained, and
(d) Comply with this Policy and Procedures Manual.

9.1.3. The VSA will analyze the types and level of sensitivity of the personal information in its custody or control.

9.2. Retention of Personal Information

9.2.1. The VSA is to keep personal information for at least one year whenever that information is used to make a decision impacting an individual. The one year period commences after its last use, or after its use was deemed to have been exhausted. [s. 31 – FIPPA].

9.2.2. If the VSA receives a request for access to personal information during the one-year retention period, the information requested must be retained for at least one year beyond the date on which the access request was closed. If the applicant receives a copy of the information and subsequently asks the Information and Privacy Commissioner to review the public body's decision on disclosure, the information must be retained for at least one year from the date on which the Commissioner makes a finding [s. 31 – FIPPA].

9.2.3. The VSA must also keep records in accordance with the applicable legislative requirements.

9.3. Removing Records from the Office

9.3.1. When working both inside and outside the office, the VSA must comply with FIPPA to protect the privacy of individuals and their personal information.

9.3.2. The staff of the VSA should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the originals left in the office.

9.3.3. The VSA follows the Privacy Commissioner's recommended procedure found in **Appendix D**.

9.4. Office Security

9.4.1. The VSA will develop reasonable safeguards to collect only the personal information that is needed for a particular purpose. If it is not needed, the VSA will not collect it [Part 3 – FIPPA].

9.4.2. Reasonable safeguards to secure confidential information include several layers of security, including, but not limited to:

(a) Risk management,
(b) Staff training,
(c) Human resources security,
(d) Technological security,
(e) Incident management, and
(f) Business continuity planning.

9.4.3. The reasonableness of security arrangements adopted by the VSA must be evaluated in light of a number of factors including:

(a) The sensitivity of the personal information;
(b) The foreseeable risks;
(c) The likelihood of damage occurring;
(d) The medium and format of the record containing the personal information;
(e) The potential harm that could be caused by an incident; and
(f) The cost of preventative measures.

9.4.4. The VSA's collection of personal and confidential information by its various departments is guided by the provisions in Appendix A.

10. Privacy Breaches

10.1. Purpose

10.1.1. All actual or suspected information incidents must be reported immediately to the Privacy Officer.

10.1.2. The Privacy Officer is solely responsible for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach.

10.2. Privacy Breaches and Information Incidents

10.2.1. A privacy breach is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by FIPPA.

10.2.2. A privacy breach is a type of information incident. Information incidents occur when unwanted or unexpected events threaten privacy or information security. They can be

accidental or deliberate and include the theft, loss, or destruction of information.

10.3. Process

10.3.1. All known or suspected privacy breaches require immediate remedial action, no matter the sensitivity of the personal information. Given the varied nature of privacy breaches, no "one-size-fits-all" response is possible, and actions are proportional and appropriate to each privacy breach.

10.3.2. The process for responding to a privacy breach is outlined in **Appendix E**. Where the privacy breach either does or is suspected to involve a breach of our technological security, the Privacy Officer ensures the VSA cyber security incident response plan has been initiated.

11. Privacy Commissioner Reviews

11.1. Right to Ask for a Review

11.1.1. A requesting person who has made a request for access to a record or a request for correction of personal information under FIPPA has the right to ask the Commissioner to review any decision, act, or failure to act of the head of the VSA with respect to that request. [s. 52 – FIPPA]

11.1.2 The Commissioner may not review decisions that the Commissioner has made in relation to records in the custody or control of the OIPC. In those circumstances, the person may request an adjudicator review the actions of the Commissioner. [s. 60 – FIPPA]

11.2. How to Ask for a Review

11.2.1. If the Privacy Officer has failed to respond to a request within the time limits required [s. 7, 10 and 11 – FIPPA], the Privacy Officer is deemed to have refused access to the record, and the time limit for requesting a review does not apply.

11.2.2. A person who does not agree with the response by the VSA to a request to access information or to correct a record may apply to the Office of the Privacy Commissioner to review the VSA's decision. A person should be referred to the website of the Office of the Privacy Commissioner https://www.oipc.bc.ca/for-the-public/how-do-i-request-a-review.aspx.

11.3. Notifying Others of the Review

11.3.1. The OIPC must provide a copy of the request for a review to the VSA and to any other person the OIPC deems appropriate [s. 54 – FIPPA.].

11.3.2 The VSA and OIPC jointly review the request to determine whether the concerns raised by the requesting person can be addressed through mediation.

11.3.3 If the VSA has any information concerning affected persons who should be notified for the review, the Privacy Officer is to convey this information to the OIPC's office as soon as possible. The VSA also relays any relevant issues, considerations, or factors that affected the outcome of the request.

11.4. Order for Severing of Records

11.4.1. The OIPC has the authority to make an order confirming that the VSA has failed to sever the records as required by FIPPA and requires the VSA to sever the records in accordance with the directions set out in the order [s. 54.1 – FIPPA].

11.4.2. An order for severing records can only be issued after the VSA has responded to the request and a request for review was received by the OIPC [s. 52 – FIPPA].

11.4.3. Any such orders should be brought to the privacy officer ASAP.

11.5. Mediation May be Authorized

11.5.1. The OIPC may appoint a mediator to investigate and to try to settle a matter under review [s. 55 – FIPPA].

11.6. Burden of Proof

11.6.1. The VSA bears the burden of proof at an inquiry into a decision to withhold or disclose information [s. 57 – BPCPA].

11.7. Duty to Comply with Orders

11.7.1. The VSA must comply with the OCPC's orders within a specified time limit unless the order has been stayed by an application for judicial review [s. 59 – FIPPA].

11.8. Enforcement of Orders of the OIPC

11.8.1. The OIPC has the right to file a certified copy of an order with the Supreme Court. Orders that are filed have the same force and effect as a judgment of that court [s. 59.01 – FIPPA].

12. Privacy Impact Assessments

12.1. Purpose of Privacy Impact Assessments

12.1.1. A Privacy Impact Assessment ("PIA") is a tool used to evaluate privacy impacts, including compliance protection responsibilities under FIPPA. PIA's promote transparency and accountability and contribute to continued public confidence in the way the government manages personal information.

12.1.2 A PIA is conducted whenever the VSA is going to instigate a new program or process, enter into an information sharing arrangement, common or integrated program, enter into a data linking initiative, implement new security measures, adopt new information technology programs or a new personal information bank, hire new contractors or similar processes or programs.[s.69(5.2) – FIPPA]

12.1.3 The Minister responsible for FIPPA issues public bodies privacy impact assessment directions, which are in **Appendix F**.

12.2. Personal Information

12.2.1. Personal information as defined by FIPPA is recorded information about an identifiable individual other than contact information. The following is a list of personal information:

(a) Name, address, email address, or telephone number;
(b) Age, sex, religious beliefs, sexual orientation, marital or family status, blood type;
(c) An identifying number, symbol, or other particular assigned to an individual;
(d) Information about an individual's health care history, including a physical or mental disability;
(e) Information about an individual's educational, financial, criminal, or employment history; and
(f) Personal views or opinions.

12.2.2. The VSA is to complete and submit a PIA even if it is thought that no personal information is involved.

12.3 What is needed to complete a PIA

12.3.1 The following may be needed when writing a PIA:

(a) Any relevant/pervious PIAs already completed around the initiative;
(b) Any legislation, other than FIPPA relevant to the initiative;
(c) Information about where data is stored, accessed, and where it flows;
(d) Security information about the data;
(e) Any records retention schedules for initiative;
(f) Any relevant research agreement; and
(g) Information about any materials required to obtain signatures.

12.3.2 The VSA has developed a PIA protocol to ensure PIA's are conducted in accordance with FIPPA requirements and the directions of the Minister. That protocol is found in **Appendix G**.

13. Information Sharing Agreements

13.1. Purpose

13.1.1. In addition to these policies and procedures, the VSA must comply with any Information Sharing Agreement or Memorandum of Understanding with other public bodies. The general form of an Information Sharing Agreement or Memorandum of Understandings is found in **Appendix H**.

13.1.2. The VSA Privacy officer is responsible for ensuring compliance with Information Sharing Agreements or Memorandums of Understanding.

13.1.3. Information Sharing Agreements (ISA) document the terms and conditions of the exchange of personal information in compliance with the provisions of FIPPA and any other applicable legislation.

13.1.4. The ISA generally includes the following information:

(a) The Parties and their contact information;
(b) The specific purpose of the agreement;
(c) A description of the personal information to be covered by the agreement;
(d) A description of how the personal information will be collected, used, and disclosed;
(e) A statement regarding the security agreements;

(f) A description of how compliance with the agreement will be monitored and investigated; and
(g) The terms of the agreement.

The provisions of FIPPA that authorize the collection, use, or disclosure of specific information are required to be listed in the applicable sections of the agreement.

13.1.5. Information Sharing Agreements are normally used when there is a regular and systematic exchange of personal information between public bodies or between a public body and an external agency (when the same information is being shared on a regular and ongoing basis).

13.1.6. Specific and non-regular requests for personal information are handled on a case-by-case basis and will be authorized by FIPPA and, where necessary, will be documented separately.

13.2 Internal Exchanges

13.2.1. The VSA will develop, where appropriate, Information Sharing Agreements to cover personal information exchanges outside the immediate program area. Personal information exchanges within the VSA do not normally require an ISA if they are for a consistent purpose [s. 33 – FIPPA] or are necessary for the performance of an employee's duties [s. 33(f) – FIPPA].

13.3 External Exchanges

13.3.1. In most cases, personal information exchanges between public bodies require an Information Sharing Agreement.

13.3.2. Given the issues regarding custody and control, an ISA might be important for instances where there are shared databases or files.

13.4 Foreign Information Exchanges

13.4.1. ISAs are required for exchanges between the VSA and another jurisdiction, even if authorized/required by legislation. A clear articulation of expectations, roles, and responsibilities is especially critical in these types of external exchanges. The VSA would be sharing personal information with a party outside the coverage of FIPPA. Before doing so, the VSA must define the conditions under which it is prepared to participate in the sharing and demonstrate a commitment to monitoring compliance over time.

14. Privacy Committee – Terms of Reference

14.1. Purpose

14.1.1. The Privacy Committee is established to monitor privacy security issues and review, identify, and implement privacy management protocols at the VSA including for the MDCCF. This will include drafting policies and procedures and the education of staff on privacy matters.

14.1.2. Privacy access requests will be dealt with by the Privacy Officer with assistance from the Legal Administrative Assistant and other staff members as necessary. The Privacy Committee may be called upon to assist the Privacy Officer in drafting access request policies and procedures.

14.2. Authority

14.2.1. The VSA is a public body subject to FIPPA. Under FIPPA and the Administrative Agreement between the Crown and the VSA dated March 24, 2004, the VSA is responsible for compliance with FIPPA.

14.3. Privacy Officer

14.3.1 FIPPA designates the Chair of the Board of the VSA as the Head of the VSA responsible for compliance with that Act. FIPPA designates the Chair of the MDCCF as the Head of that Board responsible for compliance with FIPPA.

14.3.2. Pursuant to section 66 of FIPPA, the two Chairs have delegated their responsibilities and authorities under FIPPA to the Registrar, who is also the Privacy Officer.

14.4. Members

14.4.1 The standing members of the Committee are:

1. The Privacy Officer, who will chair the meetings;
2. The Legal Administrative Assistant or Paralegal, who will represent the MDCCF, and keep the minutes, and provide administrative support; and
3. One representative from the following departments, chosen by each department annually:

    (a) Administrative
    (b) Finance
    (c) Investigations
    (d) Industry Standards

(e) Licensing
(f) Learning
(g) Consumer Services; and
(h) Communications

4. The President of the VSA may be asked to attend each meeting as necessary.

14.4.2 The representatives under paragraph 3 above are not to be from the management team.

14.4.3 Where information technology issues will be discussed, the Committee will invite someone from IT when needed.

14.5. Standing Agenda

The standing agenda for the Privacy Committee is

(a) Review of the current policies and procedures as needed
(b) Roundtable discussion on privacy and privacy security issues at the VSA and at the MDCCF
(c) Discussion on a privacy topic selected by the Committee at its prior meeting. Each member will take turns leading the discussion
(d) Education on FIPPA to be led by the Privacy Officer or another committee member
(e) Topics of interest or concern from the members of the Committee.

14.6. Meetings

14.6.1. The Committee will then meet at least once per month on dates to be set by the Committee.

14.6.2 Any member may convene a meeting where a privacy issue needs to be addressed.

14.6.3 Despite 14.6.1, if there are no topics to discuss, the Privacy Committee may elect to meet quarterly.

14.7. Sub-Committees

14.7.1. The Committee may from time to time create sub-committees for any purpose necessary to carry out the Committee's mandate. For example, a sub-committee may be established to review and develop policies and procedures in a specific topic area for review by the full Committee.

14.8. Recommendations & Approval

14.8.1. VSA - The Committee's privacy-related recommendations, including such changes or additions to any VSA policies and procedures will be brought to the Management Team by the Privacy Officer for approval. The Management Team will seek direction from the Chair of the VSA Board of Directors as necessary.

14.8.2. MDCCF - The Committee's privacy-related recommendations, including such changes or additions to any MDCCF policies and procedures, or any VSA policies and procedures that may affect the MDCCF Board, will be brought to that Board's Chair by the Privacy Officer for consultation and approval.

15. Annual Review and Audit of Privacy Policies

15.1. Develop an Oversight and Review Plan

15.1.1. The privacy officer with the assistance of the Privacy Committee will develop a plan to review and audit the privacy policies periodically.

15.1.2. The plan will set out how and when the Privacy Officer will monitor and assess the program's effectiveness against FIPPA and the public body's policies.

15.1.3. The VSA will be guided by the audit checklist developed for these reviews.

15.2. Assessing and Revising Program Controls

15.2.1. The effectiveness of program controls should be monitored periodically audited and, where necessary, revised. Monitoring is an ongoing process and should address at a minimum the following questions:

(a) What are the latest privacy or security threats and risks?
(b) Are the program controls addressing new threats and reflecting the latest complaint or audit findings or guidance of the OIPC?
(c) Are new services being offered that involve increased collection, use, or disclosure of personal information?
(d) Is training occurring, is it effective, and are policies and procedures being followed?

If problems are found, they should be documented and addressed by members of the Privacy Committee, in collaboration with the Privacy Officer.

15.2.2. For critical or high-risk processes, periodic internal or external audits can be useful in assessing the effectiveness of a privacy program. At a minimum, the Privacy Officer will conduct periodic assessments quarterly to ensure key processes are being respected.

15.2.3. Any necessary changes should be made promptly and, where critical, must be communicated to employees promptly, or otherwise throughout the ongoing training discussed above.

15.2.4. The Privacy Officer with the assistance of the Privacy Committee will review the program controls regularly and at the very least:

(a) ensure the VSA's personal information inventory is updated, and that new collections, uses and disclosures of personal information are identified and evaluated;
(b) revise policies as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices or as a result of environmental scans;
(c) treat privacy impact assessments and security threat and risk assessments as evergreen documents, so that changes in privacy and security risks are always identified and addressed;
(d) review and modify training on a periodic basis as a result of ongoing assessments and communicate changes made to program controls;
(e) review and adapt breach and incident management response protocols to implement best practices or recommendations and lessons learned from post-incident reviews;
(f) review and, where necessary, fine-tune requirements in contracts with service providers; and
(g) update and clarify external communications.

16. Video Surveillance

16.1. Purpose

16.1.1. The VSA must exercise a high degree of care when using video or audio surveillance technology in order to protect the privacy of individuals who visit or work at monitored sites.

16.1.2. The use of video and audio surveillance must be in accordance with the provisions of FIPPA.

16.2. Managing Records Created by Video Surveillance Technology

16.2.1. Records created by the VSA are covered by the Records Retention Protocol and must be retained and disposed of in accordance with approved records retention and disposition schedules.

16.2.2. Video surveillance devices that record images of individuals on tape, photographically, in digitalized format or in any other media, collect personal information that must be protected in accordance with FIPPA.

16.2.3. The VSA is to store all tapes, if not digital, not in use, in a secured locked cabinet or storage room. In addition, the VSA must securely dispose of old tapes, if used. It is recommended that the tape be shredded, burned or degaussed (magnetically erased) [s. 30 – FIPPA].

16.2.4. Records used for decision-making must be managed in accordance with FIPPA [s. 31 – FIPPA].

16.2.5. The VSA is to retain and store videotapes or digital audio-video files that are required for evidentiary purposes according to the standard procedures until they are required by law enforcement authorities.

16.2.6. A public body that uses audio-video surveillance devices for recording personal information must meet requirements set out by FIPPA, regarding the use of personal information [s. 32 – FIPPA].

16.3. Notification

16.3.1. The VSA is obligated to notify individuals affected [s. 27(2) – FIPPA]. The following is suggested wording of use in building signage:

"**This area is monitored by audio and video surveillance cameras. For further information contact:**

Contact Position
Contact Telephone number"

16.4. Implementing Video Surveillance Systems

16.4.1. It is mandatory for the VSA to conduct a PIA on any existing or planned video surveillance system [s. 69 – FIPPA].

16.4.2. The VSA, when implementing a video surveillance system to deter crime, protect the safety of members of the public and employees, or meet operational requirements, must conduct a PIA to evaluate the privacy implications of the proposed video surveillance system and to ensure that security requirements are met in the least intrusive manner possible. The Privacy Officer is responsible for conducting a PIA.

16.4.3. The decision on whether a video surveillance system is appropriate for the security requirements of a public body is based on a security threat and risk assessment, contained within the PIA.

16.5. Camera location, operation and control

16.5.1. The VSA is to ensure that the location, operation and control of any video surveillance system meet the security requirements.

16.5.2. The VSA should restrict the collection of personal information in surveillance to those purposes identified by FIPPA [s. 26 – FIPPA].

16.5.3. Within the appropriate context of those purposes, the VSA should also take into consideration whether the surveillance is a necessary and viable deterrent.

16.5.4. Access to the operation and control of any surveillance system is restricted to designated staff only.

16.6. Operational times

16.6.1. In cases where surveillance has been put in place to deal with a threat to security of individuals, assets and property, the VSA will consider the appropriateness of filming only at times where there is a higher likelihood of a threat of security to individuals, assets and property.

16.7. Audits and Reviews

16.7.1. The VSA should conduct follow-up privacy impact assessments on their use of surveillance on a regular basis in order to confirm adherence to policies and procedures and compliance with FIPPA.

16.7.2. The VSA must advise all camera operators that the system is subject to audit and that they may be called upon to justify the method of surveillance to a member of the public or an employee of the VSA, where applicable.

16.7.3. The OIPC may conduct periodic audits of the VSA's surveillance system [s. 42(1)(a) – FIPPA].

17. Website Privacy Policy Statement

17.1 The VSA is to provide a summary of its privacy policy on its website that identifies the types of personal and confidential information it collects, how it intends on using that information, and how it manages that information.

17.2 The VSA's website privacy policy statement is found in **Appendix I**.

Appendix – Forms

Important note: The excerpts included here are subject to change at any time. Readers should not rely on these excerpts without confirming whether they have been amended since publication.

A. Personal and Confidential Information Collected by the VSA

CONSUMER SERVICES

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with (witnesses).	**Personal Information:** ▪ Home address, home/cell phone number ▪ Driver's license number ▪ Date of Birth ▪ Photocopies of driver's license ▪ Power of Attorney contracts ▪ Medical information / letters from physicians **Financial Information:** ▪ Bank Statements ▪ Tax Returns ▪ Vehicle loan information ▪ Information on state of and individual's credit
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	**Commercial Information** ▪ Dealer purchase invoices (ex. how much they purchased a vehicle for)
Identify why we collect the information - how we use it.	Obtain contact information to communicate with the consumer while processing a complaint and during an investigation. Specifically: ▪ Driver's license number and Nexus information on a person's vehicle registration history aid in the identification of curbers. ▪ Power of Attorney documents help confirm that a complainant has the proper authority to file a complaint. ▪ Medical information and letters are used to inform as to whether a sale could qualify as unconscionable. ▪ Bank statements are sometimes given by consumer to prove monthly payments have come out of their account. ▪ Tax returns help determine jurisdiction to investigate if vehicle was used for business purposes.
Do we obtain direct consent to collect that information?	Yes
Where do we store that information?	▪ Files waiting to be forwarded are stored in desks ▪ Unprocessed complaint forms and awaiting documents/complaints are locked in the filing cabinet ▪ DRIVER Database
How do we secure that information?	▪ Desks and filing cabinets are locked. ▪ Access to DRIVER database is password protected with unique passwords for each individual. ▪ VSA protocol to lock out computers when person is not present at computer.

Who do we share information internally and externally?	**Internally:** Compliance, Licensing, Administration and Christina for advertising concerns. **Externally:** Dealers, consumers, complainants/complainant representatives.
When sharing information, do w share personal information such an individual's address, telepho number or bank information?	**Internally:** Generally all information is shared without redaction. **Externally:** Certain personal information is redacted when information is shared externally (e tax returns, banking information, trade secrets, dealer costs, personal email exchanges not relevant to the complaint).
When we share personal information, do we have the individual's consent or otherwis rely on legislative authority (an information sharing agreement)	The Consumer Complaint Form and Motor Dealer Response Form both make the consumer or dealer aware the information they provide will be shared, and that redactions if will be made if appropriate. **Legislative Authority:** FIPPA sections: 22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 3 and 33.3(1) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) *Business Practices and Consumer Protection Act* sections: 149 and 150. Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

INDUSTRY STANDARDS & INVESTIGATIONS

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with (witnesses).	**Personal Information:** ▪ Full names, possibly names of spouses, children, and friends ▪ Address and former address ▪ Birth date, marital status, status (First Nations identity) ▪ Telephone numbers: home, work, cell phone ▪ Email address ▪ Income sources **Financial Information:** ▪ Banking information, name of branch, co signor's data ▪ Criminal record check
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	▪ Dealer's name, registration number, address(s) ▪ Offer to Purchase identifying make, model or car being purchased/trade-in vehicle, including VIN and origin ▪ Work sheets with income ▪ Copy of DL with picture ▪ Credit application including bank account numbers, credit card numbers, tax records and pay stubs ▪ Conditional sales agreement ▪ Copy of APV9T includes registration number and driver's license numbers ▪ Past vehicle owners ▪ Sales worksheets identifying negotiation information ▪ Credit reports from Equifax, etc. includes financial data on client ▪ Financial data on vehicle, MRSP, buy in documents including purchase price, wholesale and retail prices on accessories, trade in documents. ▪ Body shop names, names of mechanics that do inspections on vehicle (repairs or structural). ▪ Salesperson/sales manager's names ▪ After sales documents: warranties, insurances etc. ▪ Health history reports/questionnaire used to obtain health and disability insurance ▪ Vehicle registration information, registration #, vehicle use, PO and RO ▪ Driver's information, license number, all vehicles registered previously in their name ▪ Copies of repair orders, with supplier's names ▪ Important documentation, Form 1, inspections ▪ Foreign driver's license numbers, passport numbers ▪ Insurance agent's names, insurance information ▪ Information from confidential sources
Identify why we collect the information - how we use it.	Information obtained is necessary to establish jurisdiction and identify if there has been a breach of the law. The nature of each complaint various and directs they type of information collected. For instance some information relates to business decisions, and make up the contents of the dealer file for the transaction. The information that is pertinent is the information that would allow us to complete the investigation of the complaint. Collect more information than needed only because it forms part of the other functions in the sale of a motor vehicle and often do not know its relevance until the investigation is complete.

Do we obtain direct consent to collect that information?	When the complainant fills out the Consumer Complaint Form, they are asked to provide consent. In respect to the information contained in the dealer's file, that is set forth in the appropriate legislation. The information obtained from ICBC is a result of an information sharing agreement at that information is an important part of completing consumer complaint investigations. There is a requirement to abide by the agreement and also by the legislation with respect to the sharing of this information.
Where do we store that information?	The information obtained during the investigation is stored both electronically and hard copy. Stored in DRIVER Database.
How do we secure that information?	▪ The hard copy files are stored in a locked filing room with entry allowed to staff only. ▪ Older files are taken off site for secure storage. ▪ Electronic files are safeguarded by password. Access to DRIVER database is password protected with unique passwords for each individual. ▪ VSA protocol to lock out computers when person is not present at computer.
Who do we share information with internally and externally?	**Internally:** Consumer services, Licensing, Administration and management as needed. **Externally:** ▪ Dealers, salespeople, by-law, CVSE, ICBC, CRA, CBSA, and financial institutions as needed ▪ Police agencies, other regulatory bodies and SIU-ICBC investigators as needed ▪ Comp Fund Board receives information from Anna ▪ Auctions, service providers, newspapers, dealer magazines, media, public, OMVIC, and AMVIC as needed ▪ With respect to an Affidavit, will provide some personal information but not banking
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	Information shared is usually contact information that is publicly available. Some information is shared with repair shops that did the work or are asked to provide an expert opinion as needed to complete an investigation. All information shared, except for with the bank, is usually for Licensing internally. When an Affidavit is completed, the accused and their legal representatives will receive necessary information if a hearing is scheduled or an undertaking is agreed to.
When we share personal information, do we have the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	▪ Have consent when sharing personal information. Rely on the legislation that is provided along with requests by police agencies (must meet FIPPA) that do not require a consumer's consent. ▪ Have ISA/MOU with ICBC and the Ministry of Finance and exchange certain specific information without a consumer's consent, as allowed by legislation. ▪ Careful not to provide information to agencies (unless police agencies conducting an investigation in which case they would be exempt) that would require consent from the consumer unless ordered by the courts. **Legislative Authority:** FIPPA sections: 22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 33(6), and 33.3(1)

	Motor Dealer Act sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) *Business Practices and Consumer Protection Act* sections: 149 and 150. Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

LEARNING

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with (witnesses).	**Personal Information:** ▪ Names ▪ Home Address/Business Address ▪ Phone Number (Personal, Cell and/or Business) ▪ Email (Personal and/or Business) ▪ Place of Employment
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	Information or a check/money order where they bank as payment for fees. Could be salesperson's or corporate (also sometimes cash payments).
Identify why we collect the information - how we use it.	Collect and use the information to register a salesperson or dealer into a class. Information is sent in via fax, email, drop off or Canada Post and is directly from the source.
Do we obtain direct consent to collect that information?	Yes
Where do we store that information?	Stored in the file room with keypad entry by staff only. Stored in DRIVER Database.
How do we secure that information?	▪ We secure the information under lock and key in a file cabinet as well as password secured in our system. ▪ Electronic files are safeguarded by password. Access to DRIVER database is password protected with unique passwords for each individual.

	▪ VSA protocol to lock out computers when person is not present at computer.
Who do we share information with internally and externally?	**Internally:** Licensing, Compliance (if they request it), Management, Accounts Payable and Administration as needed. **Externally:** Do not share information externally, only if a dealer calls to ask if salesperson is registered. This information may be given under FIPPA.
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	Share individual's address, phone number, and confirmation of Credit Card numbers if needed and consent is authorized. If a dealer calls to inquire if a salesperson is registered, it is confirmed by a yes or no as permitted to give this information. If a dealer calls to ask why a salesperson did not register for a course the dealer is told to speak with the salesperson themselves.
When we share personal information, do we have the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	Do not have the individual's consent. All sharing is internal and for a common goal (consistent purpose), i.e. to get a salesperson registered, licensed, provide a refund or take payment. **Legislative Authority:** FIPPA sections: 22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 33(6), and 33.3(1) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

COMMUNICATIONS

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with	**Personal Information:** ▪ Continuously collected for Campaigner mailing lists. This is used to send out important information (ex. bulletins, alerts, news releases) to the industry and beyond. ▪ Contacts include: all salespeople, all motor dealers, members of the board(s), VSA staff, other regulatory agency members (those who work for AMVIC/OMVIC), and various BC media contacts (Times Colonist editors).

(witnesses).	▪ Full names, work emails, personal emails, work titles, phone numbers, and addresses are collected.
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	Future plans of other regulatory agencies, etc. Frequent sales information for all of Canada from DesRosiers Automotive Consultants. Some of this information is disclosed in Annual Reports, and it is also frequently disclosed on the VSA website in the What's News. This information does not identify individual businesses and does not full into FIPPA.
Identify why we collect the information - how we use it.	Collected for Campaigner mailing lists.
Do we obtain direct consent to collect that information?	Yes.
Where do we store that information?	This information is stored in our Campaigner.com account, as well as in G Drive in Excel spreadsheets. Some of these contacts are taken straight from DRIVER, while others are given directly from the person (thereby direct consent). Stored in DRIVER Database.
How do we secure that information?	▪ Securing the information under lock and key in a file cabinet as well as password secured in system. ▪ Electronic files are safeguarded by password. Access to DRIVER database is password protected with unique passwords for each individual. ▪ VSA protocol to lock out computers when person is not present at computer.
Who do we share information with internally and externally?	**Internally:** Information is shared with all of management first before deciding to share with the rest of staff. Sometimes it is decided that the information is only for management and doesn't need to be shared with all staff. Shared on a need to know basis. **Externally:** Share information (through bulletins/alerts) with the industry (both dealers and salespeople) on an as needed basis. No personal information in Bulletins. The alerts may have contact information on an unlicensed salesperson or identity thief. This kind of information is also sent to all industry associations (such as AMVIC, ARA, NCDA) and some government officials (have contacts from government of Nova Scotia, Quebec, etc.) Also send to other organizations such as the BBB, ICBC, CarProof and Consumer Protection BC. Additionally, this kind of information is always first sent out to the Ministry to make sure it is okay to go out to the public.
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	Typically, do not share this kind of information with external or internal individuals.
When we share personal information, do we have the individual's consent or otherwise rely on legislative authority (an	Don't generally share personal information. If so, however, would need the individual's consent before giving out phone numbers, etc. **Legislative Authority:** FIPPA sections:

information sharing agreement)?	22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 33(6), and 33.3(1) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

LICENSING

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with (witnesses).	**Motor Dealer Application** **Personal Information:** Form 1A - completed by shareholder, officer or director - requires legal status, government issued photo ID (DL or passport), current residential address and addresses for the last 7 years, phone number, cell number, email, criminal record check Equifax-credit check (SIN number) birth date, past residences for 7 years, past employment for 7 years, unpaid judgments, declared bankruptcy or receivership, lawsuits or legal proceedings, convicted of a criminal offence, current investigations, judicial proceedings, copies of photo ID and legal status, criminal record check in any other jurisdiction. **Contact Information:** From 1A - work phone number, if active still at current employer, in what capacity (role). Form 1 - all contact information (phone, email, and fax) at work for the authorized spokesperson. **Salesperson Licence Application/Reinstatement** **Personal Information:** ▪ Required to supply a copy of proof of legal status (ex. birth certificate, Canadian passport, care card, citizenship card, landed immigrant visa, NEXUS card, work permit, or social insurance card) ▪ Include copy of acceptable photo identification (e.g. BC DL, citizenship card or passport if not used as proof of legal status) ▪ Criminal record check and statutory declaration and all forms of contact information for the applicant - home address, email, cell phone, alias and/or nickname or known as name ▪ Must provide employment or other activities for last five years ▪ Answer questions in relation to if applicant has been previously licensed by VSA or another regulated body and if they have had their license revoked,

	suspended or cancelled by that regulator. Must declare if they have been in violation of the *Motor Dealer Act* or *Consumer Protection Act*. If have been convicted of an offence (under name provided or another legal name or alias) for which a pardon has not been granted, under investigation or are currently charged by any law in force in Canada or elsewhere. **Contact Information:** Page 1 supplies appointed position (salesperson/dealer principal) and where they are working along with the contact info for their employment. **Employment Authorization Form** Salesperson's date of birth, email address, title and current position. **Salesperson Renewal Form** **Personal Information** ▪ Birth date, address, phone number, email – answer questions in relation to if applicant has been previously licensed by VSA or another regulated body and if they have had their licence revoked, suspended or cancelled by that regulator. ▪ Declare any new investigations, charges and/or convictions since the date of their last criminal record check. Provide credit card number, name and signature. **Contact Information:** Current employer **Form 3 – dealer change notices** Address, name and/or ownership **Form 2A/B: location/name** Spokesperson provides cell number/email **Form 3C Ownership** Provided number of shares owned by a shareholder as well as information supplied from form 1A. **Letter of Credit Release** Shareholders supply all person contact emails as well as signing request that it authorizes VSA to conduct credit check. **Dealer Renewal** ▪ Requires listing of shareholders and the amount of shares they own. ▪ If the applicant or any partner or any officer or director been convicted of any offence or been subject to any judicial proceedings under the *Business Practices Consumer Protection Act*, *Social Service Tax Act*, *Weights and Measures Act*, *Competition Act*, *Motor Vehicle Act* (moving violations excluded) or *Motor Dealer Act* or any law governing the business of motor vehicle sales in any jurisdiction in the last six years, or are there any other proceedings now pending? (Convictions need not be reported if a full pardon has been obtained) ▪ If the applicant or any partner or any officer or director been associated with any motor dealer for which the Motor Dealer Customer Compensation Fund reimbursed consumer losses? ▪ Dealership Employee List asks for names, position, date of birth ▪ Personal credit card number/name may be supplied on any of the above forms.

	▪ Salesperson criminal record witness statement; sometimes required by Manager of Licensing to supply statement in own words regarding criminal or other convictions. Lists date and type of offence, and any pertinent information such as contact information for Parole or Probation Officer.
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	▪ BC Ministry of Justice - receives RCMP Consent for Disclosure of Criminal Record Information, VSA Statutory Declaration forms contains address, date of birth and driver's license number ▪ ADESA/ICBC - notified changes to a dealership including trade name deletion or addition, change of address, dealer not occupying registered location or dealer not in good standing ▪ Equifax - credit check - name, date of birth, address and SIN ▪ AMVIC and OMVIC - salesperson enquiries regarding disciplinary action, complaints, concerns **Motor Dealer Application** **<u>Commercial and Financial Information:</u>** Business plan for a new dealer applicant includes financial statements, lease agreements, garage policy, sales projections, bank account balances and/or statements, bank account numbers, marketing plan and contact information for lawyer and accountant. **Form 1A** SIN number, birth date, past residences for 7 years, past employment for 7 years, unpaid judgments, declared bankruptcy or receivership, lawsuits or legal proceedings, convicted of a criminal offence, current investigations, judicial proceedings, copies of photo ID and legal status and criminal records check in any other jurisdiction.
Identify why we collect the information - how we use it.	Collect information for motor dealer applications, salesperson licence applications/reinstatements, employment authorization forms, salesperson renewal forms, form 3 – dealer change notices, form 3A/B location/name, Form 3C ownership, letter of credit release, and dealer renewals. Use the information to conduct credit checks and issue licenses. To Registrar who are the owners, managers and directing minds of the dealership. Know where to located salespeople.
Do we obtain direct consent to collect that information?	Yes
Where do we store that information?	All data collected/active files/historical documents are secured at the end of each business day in a locked file room. On computers data is in separate drives or G: Drive. Stored in DRIVER Database.
How do we secure that information?	▪ Through our secured network and locked file room. ▪ Access to DRIVER database is password protected with unique passwords for each individual. ▪ VSA protocol to lock out computers when person is not present at computer. Each computer must be logged onto with unique ID and password
Who do we share information with internally and externally?	**<u>Internally:</u>** Learning, Consumer Services and Compliance. **<u>Externally:</u>**

	▪ Confirmation of a Motor Dealer License application in progress and its status (if likely to be approved) with cities/municipalities in respect to the issuance of a business license. ▪ RCMP when completing criminal record checks on behalf of the VSA. ▪ RCMP and CBSA supplying background information on a dealer and/or salespeople when there is an active investigation. ▪ ADESA Auctions/ICBC to inform the status of a dealer application if no longer active. Information is limited but can include failure to occupy and not in good standing. Specifics are not provided in the notifications. ▪ Employment Agency and/or Work Safe BC to supply payment to a sponsored applicant requesting a copy of the invoice for payment. The invoice contains the personal information of the applicant (address).
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	**Learning**: Information includes current address and relevant contact information (cell number, email) in specific circumstances that may prevent a licensee from registering, attending or completing a course. Clarification of credit card number if learning is having difficulty reading the number. Payment declined may share if the same credit card was used. **Consumer Services:** Enquiring about the status of a license and why it is in that status (i.e. motor dealer license in pending). Consumer Services may need direction on a consumer inquiry and if it is a comp fund claim. Verification of a salesperson and employment history to confirm if they were employed at the time of the enquiry. **Compliance:** Enquiring about the status of a license (both motor dealer and salesperson) copy of salesperson application for interview purposes (i.e. criminal record), background on applicant including history with other regulated bodies if applicable and information on any events that may be required for review purposes. Compliance Officer reviews motor dealer application after Licensing Officer. The application contains personal information including contact and financial.
When we share personal information, do we have the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	Sharing Agreement with ICBC. **Legislative Authority:** FIPPA sections: 22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 33(6), and 33.3(1) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) *Business Practices and Consumer Protection Act* sections: 149 and 150.

	Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

ADMINISTRATION

Identify the personal and financial information collected from salespersons, consumers (complainants & claimants) and any other individuals the VSA interacts with (witnesses).	Collect Credit Card information, Criminal Record checks, Dealer and Salesperson Applications via mail, fax, courier and/or walk-in (in person).
Identify commercial and financial information the VSA collects from motor dealers or other businesses and organizations we interact with.	Collect Credit Card information, Criminal Record checks, Dealer and Salesperson Applications via mail, fax, courier and/or walk-in (in person).
Identify why we collect the information - how we use it.	Reference Licensing/Compliance/Consumer Services/Learning
Do we obtain direct consent to collect that information?	Reference Licensing/Compliance/Consumer Services/Learning
Where do we store that information?	Onsite storage: Secured filing room Offsite storage: "Security" facility Stored in DRIVER Database
How do we secure that information?	▪ Ensure the information is delivered in a timely manner from fax, mail, or walk-in, to the appropriate department. ▪ After departmental processing, ensure the information is filed and stored securely (business or personal). ▪ Electronic files are safeguarded by password. Access to DRIVER database is password protected with unique passwords for each individual. ▪ VSA protocol to lock out computers when person is not present at computer. All computers require unique log-in and password.
Who do we share information with internally and externally?	Share information internally with all VSA departments. Do not actively share information externally.
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	Will only share information within the VSA departments. This may include credit card information, personal addresses and contact phone numbers.
When we share personal information, do we have	Have consent when processing personal information (processing of credit card payments, refunds, etc.).

the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	**<u>Legislative Authority:</u>** FIPPA sections: 22(4)(c), (i), and (i); 26, 27, 33(2)(a), (b), (c), (d), (e), (h), (j), (k), and (q), 33(3)(d), 33(6), and 33.3(1) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Broker Licensing Regulation* sections: 4, 7(1), 13, 16(1) *Salesperson Licensing Regulation* sections: 3, 6(1). *Wholesaler Licensing Regulation* sections: 4, 7(1) *Business Practices and Consumer Protection Act* sections: 149 and 150. Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

Human Resources & Finance Department

Identify the personal and financial information collected from employees	Name, address, phone number, birthdate, social insurance number, banking information (direct deposits), names of dependents (benefits), health information (occasionally for accommodation purposes), tax and other statutory deductions, and salaries.
Identify why we collect the information - how we use it.	Collect information for compliance with Employment Standards Act, Income Tax Act, Income Tax Act (BC), Employment Insurance Act, Canada Pension Plan, Occupational Health and Safety Regulation, and for the provision of benefits, as well as managing operations.
Do we obtain direct consent to collect that information?	Yes.
Where do we store that information?	Locked file cabinets in HR Department and in VSA G:\\ specific to HR . Employee financial information is kept in Microsoft's Business Central (Dynamics 365) system and is shared in the ADP payroll management system and in VSA G:\\ specific to Finance.
How do we secure that information?	▪ Physical files are locked in cabinets with limited access. ▪ Access to HR's VSA G:\\ is restricted to HR personnel and the President. ▪ Electronic files are safeguarded by a unique password for each person with access. ▪ VSA protocol to lock out computers when a person is not present at their computer. All computers require unique log-in and password.

	▪ Access to financial systems (Business Central, ADP and VSA G:\\) is limited to the employees in the finance department. ▪ Confidentiality agreement with ADP as per normal terms of service. ▪ Microsoft's cyber security protocols protect data within Business Central.
Who do we share information with internally and externally?	Internally: Share information internally with the executive and management on a need-to-know basis to manage operations and deliver benefits. Externally: We will share limited and required information with our benefits provider, ADP, as well as with Canadian Revenue Agency for tax purposes.
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	Yes. On a need-to-know basis and with the consent of the employee to provide services, pay salaries, and deliver benefits to our employees.
When we share personal information, do we have the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	We obtain consent when processing personal information. **Legislative Authority:** Canada Pension Plan, RSC 1985, C-8, s. 24 Employment Insurance Act, SC 1996, c.23, s. 87 Employment Standards Act, RSBC 1996, c. 113, s. 28 Income Tax Act (Canada), RSC 1985, c. 1 (5th Supp.), s. 230 Income Tax Act (BC), RSBC 1996, c. 215, s. 58 FIPPA sections: 22(4)(c), (e), and (h); 26(d); 27(1)(f) and (4); and 33(2)(b), (c), (e), (h), (i), and (m)

B. Privacy Access Request Form

BRITISH COLUMBIA
The Best Place on Earth

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

REQUEST FOR ACCESS TO RECORDS

NAME OF PUBLIC BODY TO WHICH YOU ARE DIRECTING YOUR REQUEST			
YOUR			
LAST NAME	FIRST NAME	MIDDLE NAME	MISS MS MRS. MR. OTHER :

YOUR			
STREET, APARTMENT NO., P.O. BOX, R.R. NO.	CITY / TOWN	PROVINCE / COUNTRY	POSTAL CODE

YOUR CONTACT		
DAY PHONE NO.	ALTERNATE PHONE NO.	E-MAIL ADDRESS
( )	( )	

DETAILS OF REQUESTED INFORMATION	
INFORMATION REQUESTED (PLEASE DESCRIBE THE RECORDS YOU ARE REQUESTING. BE AS SPECIFIC AS POSSIBLE, AS THIS WILL ASSIST THE REQUEST PROCESS. ATTACH A SEPARATE SHEET IF THE SPACE BELOW IS NOT SUFFICIENT.	PLEASE SPECIFY ANY REFERENCE OR FILE NUMBER(S), IF KNOWN

ARE YOU REQUESTING ACCESS TO ANOTHER PERSON'S PERSONAL INFORMATION? YES NO
(IF SO, PLEASE ATTACH, AS APPROPRIATE:
a) THAT PERSON'S SIGNED CONSENT FOR DISCLOSURE, OR
b) PROOF OF AUTHORITY TO ACT ON THAT PERSON'S BEHALF.)

PREFERRED METHOD OF ACCESS TO RECORDS	YOUR SIGNATURE	DATE SIGNED (YYYY MMM DD)
EXAMINE ORIGINAL RECEIVE COPY		

FOR PUBLIC BODY USE

REQUEST NO.	**REQUEST INFORMATION CATEGORY**	ACCESS TO GENERAL INFORMATION (ARCS 292-30/)	ACCESS TO PERSONAL (ARCS 292-40/)

REQUEST CODE	DATE RECEIVED (YYYY MMM DD)	NAME OF PUBLIC BODY RECEIVING REQUEST

- YOU MAY MAKE A REQUEST FOR ACCESS TO RECORDS WITHOUT USING THIS FORM, PROVIDED YOU DO SO IN WRITING.
- BIRTHDATE AND CORRECTIONS SERVICE NO. ARE REQUIRED TO VERIFY THE INDIVIDUAL REQUESTING THE INFORMATION
- PERSONAL INFORMATION CONTAINED ON THIS FORM IS COLLECTED UNDER THE ***FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT***
  AND WILL BE USED ONLY FOR THE PURPOSE OF RESPONDING TO YOUR REQUEST.

C. Authorization for Release of Personal Information and Records Form

Authorization for Release of Personal Information and Records
Pursuant to section 33.1(1)(b) of the
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

I _____, being 19 years of age or older, authorize
complainant's full legal name

the Motor Vehicle Sales Authority of British Columbia (the "VSA") to disclose information, including my personal information, related to my consumer complaint to the VSA dated

_____ with respect to my dispute with
date of the Consumer Complaint Form

_____ to
name of the motor dealer

_____, so that this individual may:
third party's full legal name

☐ Enquire about the status of my complaint with the VSA;

☐ Receive copies of the correspondence from the VSA related to my complaint.

Dated this _____ day of _____, 20_____.

Complainant	Witness
Signature: _____	Signature: _____
Name: _____ *first name last name*	Name: _____ *first name last name*
	Occupation: _____

D. Procedures for Removing Records from the Office

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

PROTECTING PERSONAL INFORMATION AWAY FROM THE OFFICE

JANUARY 2015

INTRODUCTION

Whenever personal information is being used outside of the office there is an increased risk that it will be lost or compromised. Public bodies and private organizations must keep paper and electronic records safe and secure as required by the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

Whether you are traveling on a bus or plane, working from home or a remote location, or using portable devices like laptops, USB sticks, and tablets to access personal information outside the office, take the following common sense steps to reduce the risk.

GENERAL RULES OF THUMB

There are a number of things you can do to protect any personal information you remove from your office:

- Only remove personal information from the office if it is necessary to carry out your job duties.
- Take the least amount of personal information you need and leave the rest behind.
- If possible, take copies and leave the originals in the office.
- Check to see if you need management approval before removing records from the office. Your organization should have a sign-out sheet that includes your name, a description of the records, the dates the records were removed and the name of the manager who approved their removal.
- Encrypt any electronic device that stores personal information. This includes but is not limited to home computers, USB flash sticks, laptops and mobile phones.
- Avoid viewing personal information collected and used for work in public. If you must, take precautions to make sure no one else can view the personal information.
- Consider installing a privacy screen filter on your laptop screen or monitor when working outside of the office.
- Don't use your personal email as a means to transfer records containing personal information for work purposes. Refer to our Use of Personal Email Accounts for Public Business for more detailed guidance.
- Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely.

WORKING REMOTELY WITH PERSONAL INFORMATION

If you will be working with personal information from home or remotely, take care to make sure you are the only person able to access the records. Simple steps to take include:

- Log off or shut down your laptop or home computer when you are not using it
- Set the automatic logoff to run after a short period of idleness
- Do not share a laptop used for working with personal information with other individuals, including family members and friends
- When records aren't being used, store in a locked filing cabinet or desk drawer that you have sole access to
- Avoid sending personal information by email or fax from public locations
- If you are using your own device for work purposes, make sure you understand and follow your organization's BYOD (bring your own device) policy

If personal information is stolen or lost, immediately notify your supervisor and the person responsible for privacy compliance in your organization or public body, file a police report, and notify the OIPC. Your organization or public body should consider notifying the individuals whose personal information has been stolen or lost, telling them the kind of information that has been compromised and steps that are being taken to recover it.

OTHER RESOURCES

This document has benefited from a similar publication of the Office of the Information and Privacy Commissioner for Ontario, available at http://www.ipc.on.ca/images/Resources/wrkout-e.pdf

For guidelines on the Use of personal email accounts for public business, visit https://www.oipc.bc.ca/tools-guidance/guidance-documents

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867 info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy

E. Privacy Breach Protocol/Playbook

1.0 Background

Under sections 30 and 36.3 of the *Freedom of Information & Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA"), the Vehicle Sales Authority of British Columbia ("VSABC") is obliged, as a public body, to respond to breaches of privacy within their organization. This involves identifying and containing the breach, evaluating the risk of harm to the privacy of those persons to whom that personal information pertains, and reporting the breach to the affected persons and / or the privacy regulator.[1]

From a practical standpoint, this means that the following should be implemented:

- A dedicated privacy breach response protocol that complies with FIPPA and any applicable associated OIPC standards should be created and operationalized.
- VSABC needs to incorporate a formal privacy risk assessment or evaluation into their privacy breach reporting.
- VSABC also needs to determine if the risk evaluation report should be part of an existing process (such as an incident response protocol) or if it can form part of a dedicated privacy breach response protocol.
- A document suite containing templates to notify affected stakeholders in a privacy breach should be created.

  The bulk of the work in identifying, containing, and responding to a privacy breach can be implemented in a dedicated procedure and should be performed by internal stakeholders in an organization, with periodic reports given to legal counsel or the organization's privacy officer to update them on the potential exposure.

This protocol is intended to accomplish the following:

- Outline the steps in identifying, containing, and reporting a breach;
- Summarize and fulfill the legislative requirement under FIPPA to have a response protocol in place;
- Identify the internal stakeholders who need to be involved in a privacy breach response;
- Identify the stakeholders (internal and external) whose personal data may be affected by a privacy breach;
- Provide guidance on how to assess the risk of harm to privacy; and
- Provide template documents involved in privacy breach reporting and notification.

From a risk and governance perspective, this protocol was created to accomplish the following requirements:

- Formalize the process and ensure that the appropriate internal stakeholders are identified and assigned specific tasks to handle during the breach handling procedure;
- Prevent and minimize any deviations from proper procedure to ensure the process is not ad hoc;
- Create document templates that can be used to record privacy breaches;
- Create template notices to meet the mandatory breach notification requirements;

[1] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#division_d1e4345

- Triage and minimize privacy risk and potential exposure; and
- Provide legal counsel, insurers, and / or privacy regulators with documented evidence of the steps taken to mitigate risk when the privacy breach was identified.

This protocol contains appendices which may be extracted as standalone documents:

- **Appendix 1: Privacy Breach Reporting Template.** This is intended to answer questions as completely as possible when a breach is first identified and needs to be recorded.
- **Appendix 2: Breach Notification Template (Data Subjects).** This text may be used to advise affected data subjects on the details of a breach, how it may affect them, and how VSABC intends to mitigate the risk and comply with privacy breach reporting requirements. This is intended to meet mandatory breach notification requirements under FIPPA.
- **Appendix 3: Breach Notification Template (Regulator).** This may be used to advise the privacy regulator in the event of a major breach where a large number of persons are affected, and / or if a breach contains highly sensitive personal information on which the OIPC's guidance is sought. The OIPC reserves the right to investigate the matter further even after the breach has been reported and filed. This is intended to meet mandatory breach notification requirements under FIPPA.

1.1 Assumptions

The following are assumed in this protocol:

1. This SOP is triggered when a security-related or similar incident involves personal data.
2. This SOP can be customized to fit the organization's workflow and structure. Any assigned tasks or assignments can be revised for consistency and to better reflect the roles and responsibilities.
3. Any triage on the technical side does not need to be completed prior to activating the privacy breach response protocol. The two processes can run concurrently.
4. The risk matrix at Part 3.2 can be modified from time to time to more accurately reflect the types of personal data collected by VSABC, and the risks if it were in a privacy breach.
5. The roles and responsibilities in the workflow stem from the OIPC BC's guidelines for private sector organizations. In the absence of a dedicated public sector equivalent, the principles from the privacy sector are deemed to be sufficient as a baseline to establish expectations for privacy breach response.

2.0 Identify the Breach

The following types of information should be identified in a breach. This will help determine if the breach must be reported to the affected data subject and / or to the regulator in the jurisdiction. The following questions must be asked, and the responses thereto included in a privacy breach response protocol, to ensure that the correct information is captured.

2.1 What type of breach is it?

Describe the type of breach involved, as these may vary. The following are examples of privacy breaches, but it is not an exhaustive list.

- Access into a system that includes sensitive data. This may be due to a technical issue, or the user being granted permission that is not necessary.
- Sending an e-mail containing personal information to the wrong recipient. This may be due to human error.
- Employee opens a phishing e-mail. This may be attributed to human error and / or a lack of proper security awareness training.
- Major IT security incident where systems are compromised and hackers have absconded personal data and demand a ransom, often in the form of cryptocurrency.
- Sending form letters with incorrect information via mail or fax. This may result from an incorrect mail merge when drafting correspondence. For public sector and government entities who still rely heavily on traditional non-electronic mail and / or facsimile, this still occurs regularly.
- Using consumer, licensee, employee, or similar stakeholders' personal information in a live training presentation. In these situations, only dummy (non-production) data should be used, unless it is absolutely required to train an employee on the use of and orientation with an electronic system.

2.2 What caused the error?

These typically arise from one of two kinds of errors.

- Human error. Examples include:
    - Cutting-and-pasting documents and mixing up personal information, resulting in letters where documents containing the wrong information were cross-referenced to another, unrelated person(s).
    - Inputting the wrong email address and sending documents to the incorrect recipient(s).
    - Sending any other communications to the wrong recipient, including via mail and fax (the latter especially prevalent when working with public sectors that still rely heavily on facsimile).

- Technical issue. Examples include:
    - Outdated security patches
    - Backdoor entry into a system due to a vulnerability
    - Too many permissions granted to a user, including access into systems which are not necessary for them to perform their jobs
    - Spam filters not working properly, allowing spoofing e-mails to reach users in the organization masquerading as other staff members
    - DDOS attacks
    - phishing e-mail

It is important to identify the cause of the issue, so that preventative measures can be implemented. These may include providing additional training or education to staff members who caused the breach, implementing audit logs and / or regular auditing to ensure compliance, acquiring new software or other technical measures to better safeguard personal information, or running drills to educate VSABC staff on how to recognize attempted cyberattacks.

3.0 Personal Data / Risk Matrix

Not all technical breaches involve personal information, but every privacy breach involves personal data.

Privacy breaches follow the same protocol to identify and contain the breach, but not every single breach needs to be reported. This is due to the sensitivity of the personal information involved, as further explained in s. 36.3(2) of FIPPA.[2] Sometimes the personal data is minimal in terms of impact (not volume), but some can contain personal identification information that must be safeguarded and attract liability. This includes government-issued ID and genetic data.

3.1 Risk evaluation

Every breach requires an evaluation of the likelihood or risk of harm resulting from the breach. Because the likelihood of harm or similar risks will vary, all risks must be evaluated on a case-by-case basis. This is a heavily contextual test to determine what harm will likely befall an individual whose personal information has been compromised. The overriding questions[3] that must always be asked are:

- What happened?
- How *likely* is it that someone would be harmed by the breach? There is a distinction between the *possibility* or harm occurring vs. *probability*.
- Who accessed or could have accessed the personal information?
- How long has the personal information been exposed?
- Has any misuse of the personal information taken place?
- Was the information lost, inappropriately accessed, or stolen?
- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?
- Is there evidence of malicious intention to misuse the personal data?
- Has the information been exposed or disclosed to entities or individuals who are likely to attempt to cause harm or present risk to the reputation of the exposed individual(s)? (I.e., have hackers asked for ransom or threatened to publish / post the data on the internet or dark web?)
- Were several pieces of personal information breached, thus raising the risk of misuse and the complexity of the breach?
- If the affected personal data appears to be in and of itself harmless (i.e., in isolation), would that piece of information become sensitive or harmful in combination with other personal identifiers?
- Is the breached or compromised information in the hands of an individual or entity that represents a reputational risk to the individual(s)? (e.g., an ex-spouse, a colleague, or an abusive third party such as a stalker, depending on specific circumstances)
- Was the information exposed to limited or known entities who have committed to destroy, and not disclose, the data (thereby lowering potential risk)?
- Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm? (e.g., in the case of an accidental disclosure to unintended recipients)

---

[2] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section36.3

[3] Adapted as a best practice from the Office of the Information Commission for Canada: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/. The Canadian Federal OPC questions overlap with the questions asked in any robust privacy breach evaluation.

- Was the information exposed to individuals/entities who are unknown or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?
- Has harm materialized due to the exposure (demonstration of misuse)?

Consequences of a breach may include, but are not limited to, the following:

- **Identity theft:** this is particularly prevalent if identifiers such as government-issued ID (such as Social Insurance Number, driver's license, personal health care number) is involved
- **Financial loss:** this is especially likely if identity theft leads to bank fraud
- **Loss of employment:** this may be as a direct result of compromising personal files or private social media posts being shared with employers or the public, resulting in embarrassment to the person
- **Actual physical harm:** this is especially critical if a person's whereabouts are disclosed to people like to harm them physically or emotionally (such as an abusive spouse or partner or a stalker)

Generally, risk evaluation must include all the above information. A proper evaluation must always be performed by the privacy officer during the investigation stage. Section 36.3(2) outlines the types of harm as follows:

> (2) Subject to subsection (5), if a privacy breach involving personal information in the custody or under the control of a public body occurs, the head of the public body must, without unreasonable delay,
>
> (a) notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant
>
> (i) bodily harm,
> (ii) humiliation,
> (iii) damage to reputation or relationships,
> (iv) loss of employment, business or professional opportunities,
> (v) financial loss,
> (vi) negative impact on a credit record, or
> (vii) damage to, or loss of, property, and
>
> (b) notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a).
>
> (3) The head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to
>
> (a) result in immediate and grave harm to the individual's safety or physical or mental health, or
> (b) threaten another individual's safety or physical or mental health.

Remediation upon completion of proper investigation may involve additional mitigation to be completed by VSABC, such as credit monitoring or dark web monitoring.

3.2 Risk Matrix

The following is a risk matrix that lists the type of personal information collected by the organization, mapped to its sensitivity. Generally, the more sensitive the data, the more urgently you will not only notify the affected persons and the regulator, but also perform more mitigation and remediation.

The below can be modified to more accurately reflect the scope and scale of personal data collected by VSABC. It is not intended to be an exhaustive list of the types of personal data that the VSABC collects.

Category	Type(s) of Personal Data	Risk	Mitigation
1	▪ Name ▪ Business (professional) Contact Information ▪ Image / Likeness	Low	▪ None
2	▪ Date of Birth ▪ Home Address ▪ Personal Contact Information (e.g., email, phone) ▪ Marital Status ▪ Human Resource (HR) Records (e.g., compensation / benefits, vacation entitlement)	Medium	▪ Notification to affected stakeholders
3	▪ Government-Issued ID ▪ Social Insurance Number ▪ Passport / Citizenship / Immigration Documentation ▪ Driver's License ▪ Credit / Debit Card Information ▪ Financial, Banking, and Tax Information ▪ Medical and Health Data	High	▪ Notification to affected stakeholders ▪ Notification to regulator (OIPC) ▪ Credit Monitoring ▪ Dark Web Monitoring

Additional remediation may have to be performed depending upon the severity of the breach. For instance, if Social Insurance Number were compromised or stolen, that would require additional support to the affected person(s).

4.0 Containment of Breach

The first step in the triage stage of breach containment is to revoke access to the information in question. This can be accomplished by the IT security team using commonsensical steps, such as:

- Revoking access (virtual, physical, or both) for staff who have access to that information;
- Cutting off access for hackers (if possible);
- Changing access codes; and / or

- If access cannot be revoked, pulling the personal information from the active site, or making the site temporarily inactive while triage and investigation are ongoing.[4]

The technical steps should be part of the incident response protocol (IRP) to an organization. Once the IRP is activated, the privacy breach handling protocol should also be activated.

The first steps in a privacy breach handling procedure should include the following:

- Reporting incident to the privacy officer, who should open an internal file for investigation
- Designating a team member to lead the investigation of the privacy breach. This may be the privacy officer or their designate, or may even be an IT security team member who is managing the execution of the IRP
- Identifying the information that was compromised
- Preserving the evidence (the compromised evidence)
- Determine if breach is severe enough to warrant a team to manage it. This is often in the case of a large-scale breach where sensitive personal data is compromised.
- If the breach includes theft, contact police or other law enforcement to file a report
- If the breach contains particularly sensitive personal information or if a large number of individuals are affected, provide notification to the OIPC.

Ensure that the evidence is well-preserved. This is especially critical if the matter may attract criminal charges, or if an investigation is ongoing. Legal counsel, insurers, and the privacy regulator will be especially interested in assessing the damage or harm to individuals as a result of a privacy breach.

5.0 Reporting of Breach

5.1 Stakeholders

VSABC must notify the internal and external stakeholders involved in the breach. Every person who is the subject of a privacy breach is a data subject. Here is a listing of those data subjects who may need to be contacted in a breach:

Stakeholder	Interest
Consumer / Licensee	Member of the public whose personal information was compromised
Privacy Officer	Person within VSABC responsible for managing breaches, providing advice, and acting as single point of contact between regulator and organization
Privacy Consultant	External consultant who may be brought in to provide advise on and manage the breach
Legal Counsel	Assesses the legal risk and exposure to VSABC and reports up to the CEO.

[4] An example is the February 2023 Indigo data privacy breach, where the entire e-commerce platform was offline and replaced with a single message advising site visitors that they have removed the site while the investigation was ongoing. This was done to aid investigation and to prevent the site from collecting any further personal information that may be compromised.

	Manages litigation or claim if the matter reaches the courts.
Chief Information Officer	Directs the IT security team to perform technical triage
Privacy Commissioner / Regulator	Regulator to whom privacy breaches may have to be reported, especially if the breach involves sensitive personal data or numerous affected individuals. Provides advice and guidance to the organization that suffered the breach.
Police / Law Enforcement	If theft or crime is suspected
Insurer	May have to be contacted to trigger cyber-liability insurance coverage. Proper due diligence must be exercised throughout the privacy breach response, or an insurer may decline to provide coverage even if a policy is in place.
Communications	Communications team must work on corporate messaging to be delivered to the media and the public
Crisis Management	If major breach threatens existence of organization, external crisis management team may manage the entire privacy breach, from technical triage to corporate messaging and media relations, to communicating with regulator.

The above is not an exhaustive list of all stakeholders in a breach. Additionally, not every single stakeholder mentioned needs to be contacted in every situation. Only in the event of a major, catastrophic, enterprise-wide security breach here sensitive personal information is stolen and / or held for ransom would all the above parties be contacted.

5.2 Documentation

In order to properly manage a breach, an organization must have the following documentation in place to evidence the work that has been done. Precedents are included in this protocol in the appendices noted.

Document	Description	Appendix
Privacy Breach Report Template	Report to be filled out detailing the type of breach, personal data, person(s) involved, and mitigation steps in place. May be used as internal due diligence document only or given to regulator or insurer to demonstrate compliance.	1
Notification (Data Subject)	Steps to identify affected data subjects, when to notify them, and what needs to be included in any such notification, in	2

	compliance with s. 36.3 of FIPPA.	
Notification (Regulator)	Links to the EU regulators on data breach as resources and contacts.	3

The above documentation is based on the recommendations in the privacy breach response guidelines published by the Office of the Information & Privacy Commissioner of B.C.

6.0 Timeline

The following chart provides steps on how a privacy breach should be handled, and recommended guidelines on completing those steps. Additionally, approximate timelines to contain the breach are included to provide guidance on response times. Please confirm with all teams involved in breach response that the timelines for response are acceptable and can be executed by those with assigned tasks. Depending upon the circumstances and the sensitivity of the breach, timelines may be adjusted.

It should be noted that these timelines and steps are from the privacy breach response protocol the OIPC BC has published for the *private* sector.[5] Nevertheless, the operational steps in responding to the breach can be easily adapted to the public sector, in the absence of a public sector guide with similar operational steps.

#	Action	Person(s) Responsible	Timeline for Response
1	Contain the breach	Program area where breach occurred	Immediate
2	Report the breach within the organization	▪ Program area staff where breach occurred ▪ Management (report to Privacy Officer) ▪ Privacy Officer, reporting to executive as required	Same day as breach discovered
3	Designate lead investigator and appoint response team	Privacy officer	Same day as breach discovered
4	Preserve the evidence	Privacy officer	Same day as breach discovered
5	Contact law enforcement if needed	Privacy officer	Same day as breach discovered
6	Conduct preliminary analysis of risks and cause of breach	Lead investigator	Within 2 days of breach being discovered
7	Determine if breach must be reported to privacy regulator	Privacy officer	Within 72 hours of breach
8	Take further containment steps, if analysis / assessment require them	Lead investigator and / or privacy officer	Within 2 days of breach

[5] Office of the Information & Privacy Commissioner for British Columbia, "Privacy Breaches: Tools and Resources for the Private Sector": https://www.oipc.bc.ca/guidance-documents/1428 (February 2023).

9	Evaluate risks associated with breach	Lead investigator and / or privacy officer (possibly with legal)	ASAP
10	Determine if notification to affected individual(s) is required	Privacy officer	Within 72 hours of breach
11	Notify affected individuals (consumers, licensees, and regulator) in writing	Privacy Officer or program area manager	Within 72 hours of breach
12	Contact others as appropriate	Privacy Officer or program area manager	As needed
13	Determine if further in-depth investigation is required	Privacy Officer or program area manager	Within 2-3 weeks of breach
14	Conduct further investigation into cause and extent of breach if necessary	Privacy Officer, CIO / CISO, external investigator, IT security auditor	Within 2-3 weeks of breach
15	Review investigation findings and develop prevention strategies	Privacy Officer or program area manager	Within 2 months of breach
16	Implement prevention strategies	Privacy Officer or program area manager	Dependent upon strategy
17	Monitor prevention strategies	Privacy Officer, program area manager or CIO/CISO	Annual privacy / security audits

The above timeline is modified from the Office of the Information & Privacy Commissioner for British Columbia's guidelines on handling privacy breaches.[6]

[6] "Privacy breaches: tools and resources for the private sector": https://www.oipc.bc.ca/guidance-documents/1428 (February 2023).

Appendix 1 – Privacy Breach Report Template

This privacy breach report template is based on the guideline “Privacy Breaches: Tools & Resources”, published by the Office of the Information & Privacy Commissioner of British Columbia. While it is a best practice resource, it is not intended to supersede, replace, or override templates from other jurisdictions, including GDPR. If an organization operates in a jurisdiction that mandates very specific reports to be filed using their precedents, those should be used in place of this template report.

It must be noted that this form can be customized into a format specifically for internal reporting only. Not all privacy breaches need to be reported to a regulator, but as a due diligence measure, internal reports of privacy breaches and how they were handled should be maintained.

The attached document may be cut-and-pasted in its entirety in a standalone document.

[THE REST OF THIS PAGE IS LEFT INTENTIONALLY BLANK.]

Date of Report	
Contact Information	
Name	
Title	
Phone / Fax / Email	
Mailing Address	

Risk Evaluation	
Incident Description	
Describe the nature of the breach and its cause	
Date of Incident	
Date Incident Discovered	
Location of Incident	
Types of Individuals (Data Subjects) Affected	☐ Consumer ☐ Licensee ☐ Third Party ☐ Employee ☐ Government ☐ Other (please describe):
Describe the type of Personal Information Involved (name, address, government-issued ID, finar medical). Provide description **only (Refer to Risk M 3.1, or chart at end of this report).**	
Describe the physical security measures in place (l alarm systems, etc.)	
Describe the technical safety measures	☐ Encryption ☐ Password ☐ Other (please describe):

Describe training and education measures in organization	☐ Online Course ☐ Live Training ☐ Continuing education seminars ☐ Other (please describe):

Incident Description – Harm from the Breach	
Identify the type of harm which may result from this breach	
Identity Theft Description: loss of government issued ID, credit / d card number, driver's license number, personal he number, financial information, passwords	
Risk of Physical Harm Description: Does disclosure of the personal informa put an individual at risk of physical harm (e.g., sta or harassment)	
Hurt, Humiliation, Damage to Reputation / Brand Description: Associated with the loss of medical mental health records, disciplinary records, pers correspondence, sensitive images	
Loss of Business / Employment Opportunities Description: Usually as a result of damage t reputation or an individual	
Breach of Contractual Obligations Description: Contract provisions may require that in event of a data loss or privacy breach, affected parties must be notified	

Future breaches due to similar technical failures Description: Notification to manufacturer may necessary if a recall is warranted and/or to preve future breach by other users	
Failure to meet professional standards or certifica standards Description: Notification may be required t professional regulatory body or certification author	
Other Harms (please describe)	

Notification	
Have you notified your privacy officer?	☐ Yes – Who and when: ☐ No – Why not, and when will they be notified:
Have policy, authorities, and/or professional bodie persons been contacted?	☐ Yes – Who and when: ☐ No – Why not, and when will they be notified:
Have affected individuals been notified? *(See next section on Notification to Individuals fo questions that must be answered for a full evaluati*	☐ Yes – Manner of Notification, and how many affected? ☐ No – Why not?
What information was included in the notification:	☐ Date of breach ☐ Description of breach ☐ Description of personal information inappropri accessed, collected, used, or disclosed ☐ Risk or harm to the affected individual(s) cause the breach ☐ Steps taken so far to control or reduce the harm ☐ Future steps planned to prevent further pri

	breaches ☐ Steps individual can take to reduce harm ☐ Contact information for the privacy commissione ☐ Organization contact information for fur assistance

Evaluation of Notification Requirement – Affected Individuals	
Consideration	*Check if Applicable (add Notes)*
1. Legislation requires notification. ▪ Are you or your organization covered legislation that requires notification of affected individual? ▪ If you are uncertain, contact the Informa and Privacy Commissioner.	
2. Contractual obligations. ▪ Do you or your organization have a contra obligation to notify affected individuals in case of a data loss or privacy breach?	
3. Risk of identity theft. ▪ Is there a risk of identity theft? ▪ How reasonable is the risk? Guidance: Identity theft is a concern if the br includes unencrypted information such as name conjunction with social insurance numbers, credit numbers, driver's licence numbers, personal he numbers, debit card numbers with passv information and any other information that can be for fraud by third parties (e.g., financial).	
4. Risk of bodily harm.	

▪ Does the loss of information place individual at risk of physical harm, stalkir harassment?	
5. Risk of hurt, humiliation, damage to reputation. ▪ Could the loss of information lead to humiliation or damage to an individ reputation? Guidance: This type of harm can occur with the lo information such as mental health records, me records, or disciplinary records.	
6. Loss of business or employment opportunities. ▪ Could the loss of information result in dar to the reputation to an individual, affe business or employment opportunities?	

Contacting the Privacy Commissioner
Should the regulator be contacted? Consider the following details:
▪ Is the personal information sensitive? ▪ Is there a risk of identity theft or other harm, including pain and suffering, or loss of reputation to affected individual(s)? "Significant harm" includes but is not limited to: bodily harm, humilia damage to reputation / relationships, loss of employment / business / professional opportun financial loss, negative impact on a credit report, or damage to / loss of property. Also consider i disclosure of personal information would result in immediate and grave harm to a person (inclu harm to them physically or to their mental state), or if it would threaten another person's physi or psychologically. ▪ Have a large number of individuals been affected by the breach? ▪ Has the disclosure created a real and significant risk of harm to the affected individual that may c their health or safety to be compromised? Examples may include but not be limited to: doxing (h address to internet trolls or people threatening physical harm), stalking or harassment (especia the person has an actual stalker or an abuse former partner) ▪ Has the information not been recovered? ▪ Did the breach occur from a systemic or technical issue?

▪ Has a similar breach occurred in the past? ▪ Does your organization need assistance in responding to the breach?
If reporting this breach to the commissioner, include a copy of the notification letter. Please contact l counsel to ensure that the notification is approved.

Prevention	
Describe the immediate steps taken to contain reduce the harm of the breach (e.g. locks chan computer access codes changed or revoked, compu systems shut down).	
Describe the long-term strategies you will tak correct the situation (e.g. staff training, p development, privacy and security audit, contra supervision strategies, improved technical sec architecture, improved physical security).	
If a security audit or incident investigation report have been completed, please include a copy with notification. This may be required by the regulator. Please advise the Chief Information Officer of san	

Reference: Risk Matrix

Categor	Type(s) of Personal Data	Risk	Mitigation
1	▪ Name ▪ Business (professional) Contact Information ▪ Image / Likeness	Low	▪ None
2	▪ Date of Birth ▪ Home Address ▪ Personal Contact Information (e.g., email, phon ▪ Marital Status ▪ Sexual Orientation / Gender Identity ▪ Human Resource (HR) Records (e.g., compensa / benefits, performance reviews, vacation entitlement)	Mediu	▪ Notification to affected stakeholders

3	▪ Government-Issued ID ▪ Social Insurance Number ▪ Passport / Citizenship / Immigration Documentation ▪ Driver's License ▪ Credit / Debit Card Information ▪ Financial, Banking, and Tax Information ▪ Medical and Health Data	High	▪ Notification to affected stakeholders ▪ Notification to regulato (OIPC) ▪ Credit Monitoring ▪ Dark Web Monitoring

Appendix 2 – Breach Notification Letter Template (Data Subjects)

Vehicle Sales Authority of British Columbia
8029 - 199 Street, #280
Langley, BC V2Y 0E2

Dear [**name**]:

I am writing to you with important information about a recent privacy breach involving your personal information. The Vehicle Sales Authority of British Columbia first became aware of this breach on [**date**]. The breach occurred on or about [**date**] and occurred as follows:

[DESCRIBE THE EVENT, INCLUDING, AS APPLICABLE, THE FOLLOWING:]

- A brief description of what happened.
- Description of the information that was inappropriately accessed, collected, used, or disclosed (e.g., full name, Social Insurance Number, date of birth, home address, account number(s), government-issued identifier, etc.).
- Risk(s) to the individual caused by the breach. Refer to the Risk Matrix to confirm the risk involved due to the exposure of the personal information.
- Steps the individual should take to protect themselves from potential harm from the breach.
- A brief description of what the Authority is doing to investigate the breach, control or mitigate harm to individuals and to protect against further breaches.

[Sample paragraphs regarding credit protection, if credit card information was compromised. This needs to be discussed at a high level within the Authority, as credit monitoring will incur additional costs. If the personal information involves potential fraud, the Authority may wish to also consider dark web monitoring.]

- To help ensure that this information is not used inappropriately, the Authority will cover the cost for you to receive credit monitoring for one year. To receive this credit protection service, please provide your consent by calling our toll-free number at [fill in number here].
- **You may periodically request a credit report**. Whether or not your data has been involved in a breach, you can receive a report from each of the national credit bureaus listed below. You should remain vigilant about suspicious activity and check your credit reports, as well as your other account statements, periodically over the next 12 to 36 months. You should immediately report any suspicious activity to the credit bureaus.
- **You may place a fraud alert on your credit report.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. This can help prevent an identity thief from opening additional accounts in your name. As soon as one of the credit bureaus confirms your fraud alert, the other credit bureau will be automatically notified in order to place alerts on your credit report, and the reports will be sent to you free of charge. To place a fraud alert on your credit file, contact one of the two national credit bureaus at the numbers provided below.

- **Order your credit reports.** By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- **You can place a "credit freeze" on your credit file** so that no credit reports can be released without your approval. Please contact the national credit bureaus below for more information. Both bureaus charge a fee for this service. To contact the credit bureaus, you can call the numbers below, or you can visit their websites for further contact information:
    - Equifax: 1-800-465-7166; www.equifax.ca
    - TransUnion: 1-800-663-9980; www.transunion.ca
- **Continue to monitor your credit reports.** Even with a fraud alert on your account, you should continue to monitor your credit reports to ensure that an imposter has not opened an account with your personal information.

A toll-free number is available for you to call us with questions and concerns about the loss of your personal information. You may call [**insert toll-free number**] during **normal business hours** with any questions you have.

We have also established a section on our website [**insert link**] with updated information and links to resources that offer information on what to do if your personal information has been compromised.

We take our role in safeguarding your personal information and using it in an appropriate manner very seriously. Please rest assured that we are doing everything we can to rectify the situation.

Please note that under the *Freedom of Information & Protection of Privacy Act*, RSBC 1996, c. 165, you are entitled to register a complaint with the Office of the Information & Privacy Commissioner of British Columbia with regard to this breach. Complaints may be forwarded to the following:

> Office of the Information and Privacy Commissioner for British Columbia
> PO Box 9038 Stn. Prov. Govt.
> Victoria B.C. V8W 9A4
> Telephone: (250) 387-5629
>
> Callers outside Victoria can contact the office toll-free by calling Enquiry BC at 1-800-663-7867 and requesting a transfer to (250) 387-5629.

Additional information is available on the Privacy Commissioner's website at http://www.oipc.bc.ca.

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to communicate with the undersigned.

Sincerely,

[**Insert applicable name and contact information**]

Appendix 3 – Breach Notification (Regulator)

VSABC should notify the OIPC of a privacy breach through their online reporting mechanism located at https://www.oipc.bc.ca/resources/report-a-privacy-breach/. The OIPC should be notified if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph 36.3(2).[7]

At minimum, the OIPC BC will want to see the following information if or when VSABC notifies them of a data breach:

Type of Data Breach	The consequences of, for example, sensitive data leaking to the internet can be different to those of not being able to access your personal data due t information system malfunction.
Nature, Sensitivity, Amount of Personal Dat	The more sensitive the data affected by the personal data breach, the greate risk to the persons concerned. A combination of different data types on the subject is frequently more sensitive than a single data item. When a personal breach affects a large group, so will the consequences.
Ease of Identification	It is important to assess how easily the data subjects can be identified from materials affected by the personal data breach, either directly or indirect combination with other data. Identifiability can be influenced by how well the has been encrypted or pseudonymized, among other things.
Attributes of the Subject	Personal data breaches can have more serious consequences when they involv children or others in a vulnerable position.
Attributes of the Contr (VSABC)	The sector and role of the controller can have an impact on the severity of the caused by the personal data breach. For example, if the personal data breach occurs in the patient record system of a hospital, the threat to the data subjec will probably be greater than if it had taken place in a newspaper's subscriber register.
Severity of Consequences of the Br	The consequences of a personal data breach can be considered particularly se if it can result in identity theft, fraud, anxiety, humiliation, or loss of reputatio The party that gained access to the information can also affect the consequen that can be expected. The likelihood of misuse can be greater if it is known tha the data fell into the hands of a criminal, for example. When assessing the risk involved in a personal data breach, take the severity a probability of the possible consequences into account. The risk related to a personal data breach is the greater, the more severe and probable the consequences for individuals.

[7] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section36.3

F. Minister's Directions to Public Bodies on PIA

PRIVACY IMPACT ASSESSMENT DIRECTIONS

TO:	HEADS OF ALL PUBLIC BODIES THAT ARE NOT MINISTRIES
DIRECTION:	2-21
SUBJECT:	Directions to heads of public bodies that are not ministries on conducti privacy impact assessments
AUTHORITY:	These directions are issued under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*.
APPLICATION:	These directions apply to heads of all public bodies that are not ministri
EFFECTIVE DATE:	November 26, 2021

Honourable Lisa Beare
Minister of Citizens' Services

Minister of Citizens' Services

Directions to Heads of Public Bodies that are Not Ministries

issued under Section 69 (5.3) of the

Freedom of Information and Protection of Privacy Act

I, Lisa Beare, Minister of Citizens' Services (the Minister), issue the following directions to heads of public bodies that are not ministries, hereafter referred to as "public bodies", under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the Act).

These directions repeal and replace Direction 1/14 issued May 9, 2014.

A. Preamble

Relevant Legislative Requirements

Section 69 (5.3) of the Act requires the head of a ministry to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

Purpose

The purpose of these directions is to:

1. Direct public bodies in determining when a PIA must or may be conducted.
2. Direct public bodies in conducting and documenting a PIA that will:
    a. Determine whether their initiative meets or will meet the requirements under Part 3 of the Act; and
    b. Identify and assess privacy risks and identify a risk response(s) that is proportionate to the level of the risk.

B. Definitions

In these directions:

"common or integrated program or activity" has the same meaning as in the Act;

"data-linking program" has the same meaning as in the Act;

"head" has the same meaning as the head of a public body that is a not a ministry in Schedule 1 of the Act;

"initiative" means an enactment, system, project, program, or activity;

"ministry" means a ministry of the government of British Columbia;

"personal information" has the same meaning as in the Act;

"privacy impact assessment (PIA)" has the same meaning as in the Act;

"privacy risk" includes:

- an inherent risk of unauthorized collection, use, disclosure, or storage of personal information; and
- something that may inappropriately override or otherwise limit personal privacy.

The level of risk may vary based on:

- the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information; and, • the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information.

"public body" means a public body as defined in the Act that is not a ministry; and,

"service provider" has the same meaning as in the Act.

C. When a PIA must or may be conducted

1. A head of a public body must conduct a PIA on a new initiative for which no PIA has previously been conducted.

2. A head of a public body must conduct a PIA before implementing a significant change to an existing initiative, including but not limited to a change to the location in which sensitive personal information is stored, when it is stored outside of Canada.

3. Where a head of a public body is not required to conduct a PIA by items 1-2, above, they may conduct a PIA at their discretion and in accordance with these directions.

D. General Directions on conducting a PIA

When conducting a PIA for an initiative, the head of a public body must do the following:

1. Identify the purpose or objective of the initiative.

2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.

3. Where applicable identify:
    a. how and from whom the personal information will be collected;
    b. how the personal information will be used;
    c. how and to whom personal information will be disclosed; and
    d. if an assessment or disclosure for storage of personal information outside of Canada is required, as per E.

4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.

5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.

6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.

7. The head of a public body may document the PIA using a template created by the Minister responsible for the Act or an appropriate format as determined by the head of the public body.

8. Designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative.

9. In addition to the requirements outlined in Directions D1 to D8, identify if a supplementary assessment (E1 to E5) of disclosure for storage of personal information outside of Canada is required for an initiative by determining:
    a. whether the initiative involves personal information that is sensitive; and,
    b. if the personal information that is sensitive is disclosed to be stored outside of Canada.

Where applicable, the head of the public body must confirm their adherence in the PIA to the following requirements under Part 3 of the Act:

10. Confirm that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act;

11. Where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;

12. Confirm that a process is in place, per section 29 of the Act, to correct individuals' personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;

13. Where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act;

E. Directions on a supplementary assessment of disclosure for storage of personal information outside Canada

1. If the conditions in D9 are not met, or the disclosure outside of Canada is made in accordance with section 33 (2) (f), an assessment of disclosure for storage of personal information outside of Canada is not required.

2. If both conditions in D9 are met, then an assessment of disclosure for storage of personal information outside of Canada is required.

3. If an assessment of disclosure for storage of personal information outside of Canada is required, the head of a public body must identify the privacy risk(s) as well as the level of the privacy

risk(s) associated with the disclosure by examining factors which include but are not limited to the following:

a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
c. whether the personal information is stored by a service provider; and,
d. where the personal information is stored.

4. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).

5. The outcome of the assessment of disclosure for storage of personal information outside Canada will be a risk-based decision made by the head of the public body on whether to proceed with the initiative, considering E3 and E4.

G. PIA Protocol

1.0 Background

This document is a draft policy governing how the Vehicle Sales Authority of BC ("VSABC") governs the use of privacy impact assessments ("PIA"), and how they intend to fulfill their legislative obligations (under s. 69(5.3) of the *Freedom of Information & Protection of Privacy Act*, RSBC 1996, c. 165) by incorporating a PIA into the overall due diligence and procurement cycle. This PIA policy was created as part of the overall policy pack Kobalt is delivering to VSABC as part of the privacy compliance exercise.

In addition to the PIA policy, Kobalt has created an optional PIA Questionnaire (attached in Part 3.0) as an additional supporting document. The purpose is to have an additional due diligence measure to pre-screen any data-linking initiatives or common / integrated programs at a high level for any privacy risks, and to determine if a full PIA is required.

2.0 PIA Policy

In addition to the pre-existing PIA template, it is recommended that VSABC also implement a PIA policy as a guidance document. This policy is based upon the Privacy Impact Assessment Direction #2-21, issued in September 2021 by the Province of British Columbia.[8] This is intended to accomplish the following:

- Creating an internal governing document that compels the completion of a PIA, using defined triggers to ensure that a PIA is done as part of a formal workflow;
- Aligning VSABC privacy practice with Provincial BC government requirements on PIAs;
- Incorporating PIAs into the overall business activities of VSABC (e.g., during procurement cycle)
- Ensuring that privacy by design elements are examined, accounted for, and built into initiatives, programs, and projects within VSABC;
- Identifying all stakeholders within VSABC that need to know about the privacy risks are consulted and their approval of (or declining of) these risks are formally evidenced; and
- Demonstrating that privacy governance starts at a high level and ensuring that anyone acquiring or building a system within or for VSABC adheres to these requirements.

Completion of a PIA is often a strict requirement in the procurement cycle for public bodies. Therefore, having a governing document would help ensure that VSABC complies with procurement rules.

The PIA policy should be posted internally within VSABC and accessible to all employees. Anyone in the organization who is responsible for building / acquiring a system or managing a project involving personal information must familiarize themselves with this policy and ensure they comply with it. Examples of these personnel may include the following:

- Privacy: responsible for updating the PIA policy and overseeing the PIA process
- IT Security: when implementing a system involving PI
- Procurement: when acquiring a system on behalf of VSABC that involves PI
- Human Resources: when using or migrating employee PI in a new system
- Legal: for due diligence and compliance purposes

[8] https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/directions/2021_pia_directions_for_non_ministries_-_final.pdf

- Marketing / Communications: when creating a marketing campaign involving PI from respondents / participants

The full text of the draft PIA policy appears at the next page. This can be appended to the full PIA template document as a resource. The draft text can be retrofitted into any pre-existing policy templates VSABC uses.

2.1 Privacy Impact Assessment Policy

1.0 Introduction

A privacy impact assessment (PIA) is a due diligence document designed to examine the impact of collecting, using, disclosing, and storing (retaining) personal information pertaining to VSABC's stakeholders, employees, and third parties. A PIA is an in-depth examination of how VSABC identifies privacy risks, any mitigation thereof, and the acceptance of such risks. This is done in compliance with s. 69.5 of the *Freedom of Information & Protection of Privacy Act*, RSBC 1996, c. 165. ("FIPPA").

2.0 Purpose

A PIA is intended to be a due diligence exercise to ensure that VSABC's business activities are compliant with applicable privacy legislation.

The Office of the Information & Privacy Commissioner for British Columbia (OIPC) published a Direction on the use of PIAs in the public sector. Specifically:

Purpose

The purpose of these directions is to:

1. Direct public bodies in determining when a PIA must or may be conducted.

2. Direct public bodies in conducting and documenting a PIA that will:

a. Determine whether their initiative meets or will meet the requirements under Part 3 of the Act; and

b. Identify and assess privacy risks and identify a risk response(s) that is proportionate to the level of the risk.

If in doubt, please check with the VSABC privacy officer to confirm the legislative requirement for completing a PIA for your initiative or project.

3.0 Policy Statement

VSA is committed to the protection of personal information. We endeavour to assess the collection, use, disclosure, and retention of personal information to ensure compliance with applicable data privacy protection legislation (namely, FIPPA).

When planning a new project or making any substantive changes to existing systems that materially

affects the collection, use, disclosure, and storage of personal information, the business group responsible for the system or project shall advise the VSABC privacy officer of such a change. The VSABC privacy officer may then determine if completing a PIA is necessary.

This PIA policy will apply to any “common or integrated program” or “data-linking initiative” as defined in FIPPA. For certainty, the legislative definitions are as follows:

"common or integrated program or activity" means a program or activity that

(a) provides one or more services through
(i) a public body and one or more other public bodies or agencies working collaboratively, or
(ii) one public body working on behalf of one or more other public bodies or agencies, and

(b)is confirmed by regulation as being a common or integrated program or activity;

"data-linking program" means a program of a public body that involves data-linking if at least one data set in the custody or under the control of a public body is linked with a data set in the custody or under the control of one or more other public bodies or agencies without the consent of the individuals whose personal information is contained in the data set;

All business groups shall commit to working with the VSABC privacy officer, IT security, legal, and other business groups or stakeholders to complete a PIA prior to the acquisition of a solution or the launch of a new project.

4.0 Policy Outcomes

All business groups will provide the resources necessary for the VSABC privacy officer to complete the PIA. This includes but is not limited to documentation, financing, technical capability, and time.

A PIA must be completed on all data-linking initiatives and common or integrated programs, as defined in FIPPA. This includes all net-new systems, projects, technologies, or services involving personal information. The PIA must include any mitigation or remediation necessary to minimize the impact of privacy risk. The VSABC privacy officer and designated personnel must sign off on the PIA prior to the launch or acquisition of the project or initiative. A PIA may be performed retroactively if a legacy system or other program / initiative had been approved without a formal PIA having been previously completed.

Any high-risk activity or issues identified in the PIA must be resolved prior to the launch or acquisition of a system or project. If appropriate, the VSABC privacy officer may provide preliminary approval and place conditions on the use of the system or project even if a PIA is not yet fully completed. However, the VSABC privacy officer reserves the right to revoke preliminary approval if a project is deemed to be too high-risk to VSABC or if the activity is not compliant with the applicable privacy legislation.

If an identified risk cannot be resolved or mitigated, that risk must be identified by the privacy officer, entered into the VSABC risk registry, and signed off by the CEO.

5.0 Application

This policy applies to all IT security solutions built by or acquired by VSABC, and to any initiative or project involving personal information. This policy applies to all business groups within VSABC. If a system does not require a PIA, then the business group seeking exemption must obtain express consent from the VSABC privacy officer and / or their delegate.

6.0 Requirements for PIA

A PIA may be required for one or more of the following scenarios.

1. At the start of or prior to the launch of any common or integrated programs.
2. At the start of or prior to the acquisition, creation, or launch of data-linking initiatives, such as:
    a. Proposed acquisition of a new system that may involve personal information (e.g., accounting software, client file management, payroll, etc.). This also includes any systems for which VSABC is acquiring a user license, or where a third-party service provider stores personal information in their environment (e.g., in a cloud-based storage solution).
    b. Proposed building of technology or software where personal information may be stored. This applies to purpose-built in-house tools and to any systems that are customized for use by VSABC.
3. Any new or increased collection of personal information, either with or without the consent of individuals.
4. Any shift from direct to indirect collection of personal information from individuals.
5. New sharing of personal information between programs within VSABC or with third parties, including service providers, government, law enforcement, or any public entities with whom VSABC may partner.
6. Any proposal where personal information previously collected, used, disclosed or stored for a specific purpose is to be collected, used, or disclosed for another (secondary) purpose. For example, using client personal contact information for marketing purposes – which is not the purpose for which the personal information was collected – triggers a PIA.
7. Data warehousing proposals require a PIA to ensure that the third-party hosting solution complies with privacy legislation.
8. Sharing client or employee with third parties through outsourcing, contracting, or alternative service delivery models (through either a common or integrated program or through a data-linking initiative).
9. Any major changes to security mechanisms that affect the access to and control of personal information of VSABC clients or employees.
10. Any planned significant change to policies, business processes, or systems that may affect the location of data or personal information within a system or group of systems.
11. Any reconfiguration, consolidation, re-engineering, or change in functionality resulting in access to personal information (through systems or technology) for new business groups, partners, or third parties.
12. Disclosure of personal information outside of Canada, through the use of third-party service providers or vendors.
13. Any order from the OIPC to complete a PIA as per the September 2021 direction.

If you are uncertain if a specific project or activity requires a PIA, check with the VSABC privacy officer prior to acquiring or building a system or solution or starting a campaign that involves personal information.

7.0 PIA Questionnaire

Prior to the completion of a PIA, the project owner or sponsor must first complete a PIA Questionnaire. This document is intended to accomplish the following:

- Provide the VSABC Privacy Officer and other internal stakeholders with a preliminary high-level review of the project or solution before a formal PIA is conducted;

- Act as a "screening" document that would, subject to the decision of the VSABC Privacy Officer and / or other stakeholders (e.g., the privacy regulator), stand in the place of a formal PIA if it is determined that the privacy risks are low; and
- If used to stand in the place of a full PIA, shorten the due diligence process when acquiring a SaaS solution or starting a project or initiative that requires personal information.

8.0 Roles and Responsibilities

Role	Responsibility
Privacy Officer	Oversees the entire PIA process, including drafting, review, discussion with rel stakeholders, and consultation with regulators as required. Identifies risks and raises to the attention of the executive or legal counsel. Responsible for updating this PIA p
Work Unit Manager	Works with Privacy Officer and makes available all relevant documentation with whic Privacy Officer can draft and review a PIA.
Systems Management / Secu	Determines if there is an IT security-related risk in the project or initiative. Condu security threat risk assessment as required to cover off technical evaluation of the pro
Legal Counsel	Consults with the Privacy Officer if the privacy risks may also result in a foreseeable risk to the organization. NB: This only applies if the Privacy Officer and Legal Couns not the same person.

9.0 Monitoring and Compliance

The VSABC privacy officer is responsible for the following:

- Determining if a PIA is required;
- Monitoring all PIA progress, including any prospective, in-flight, completed, abandoned, and / or revised PIAs;
- Determining if conditions for approval (e.g., steps for mitigation or additional review) need to be placed on a PIA prior to the launch of the project or service, to stand in the place of full and final approval of the project or service;
- Identifying instances where a PIA needs to be revised (in the form of a revision, addendum, or other similar document) if the way a system or project processes personal information has been substantively changed;
- Contacting the OIPC if required to obtain advice or guidance on a particularly complex program or data-linking initiative; and
- Revising this Policy and the PIA template as required.

10.0 Policy Approval & Review

This policy was approved by:

VSA BC Privacy Officer	Patrick Poyner
Version / Date	1.0 / [date]

3.0 PIA Questionnaire

A preliminary pre-PIA privacy assessment document or a similar questionnaire would serve the following functions:

- Provide the VSABC Privacy Officer and other internal stakeholders with a preliminary high-level review of the project or solution before a formal PIA is conducted;
- Act as a "screening" document that would, subject to the decision of the VSABC Privacy Officer and / or other stakeholders (e.g., the privacy regulator), stand in the place of a formal PIA if it is determined that the privacy risks are low and a full PIA is not required; and
- If used to stand in a place of a full PIA, shorten the due diligence process in the procurement cycle, thereby creating organizational efficiencies.

The following section contains a draft PIA questionnaire that may be used as part of the overall PIA review cycle. This is subject to any other outstanding questions or concerns that the VSABC Privacy Officer requires for the screening document. It should be noted that **no** legislative analysis is performed in the Questionnaire. This work should be performed by the VSABC Privacy Officer. If VSABC decides to implement this document, it should be referenced in the PIA Policy (see Part 2.1, #7).

3.1 PIA Questionnaire Template

This PIA Questionnaire is to be completed as directed by the VSABC Privacy Officer. Please answer all of the following questions with respect to the project or initiative you are sponsoring and submit this to the Privacy Officer. Completion of this PIA Questionnaire does **not** automatically mean that your project is compliant with applicable privacy legislation.

Project Overview	
Name of Project	
Project Sponsor / Owner	
Department / Business Group	
Is Project Outsourced? (Y/N)	
Is Project Enterprise-Built? (Y/N)	
Vendor(s)	

List all vendors including the developer, any outsourced suppliers and subcontractors who are supporting the proj	
List vendor location. Include the country(-ies) where the will be hosted.	
Is this a cloud-hosted solution hosted by the vendor? (Y/I	
Will VSABC or a vendor be hosting the solution? (Y/N)	
Why are we using this solution as opposed to an alternati vendor or solution?	

Personal Information (PI) Inventory	
From whom is the PI being collected? List all **sources** of by type. E.g., client, client representative, government or public b third-party vendor, law enforcement, etc. If in doubt: list the party supplying the PI	
List all **types** of PI. E.g., name, home address, personal contact information (email & phone), DOB / age, government-issued ID (e.g. Passport, Driver's License, Social Insurance Number), financial records, marital status, health information, residency, citizenship, criminal record / history, photos / likeness (including voice or video recordings), opinions, sexual orientation, religion, political / philosophical belie banking & financial information, employment informatic (such as compensation or benefits) The above is **not** an exhaustive list of types of PI.	
Will the PI collected be aggregated, de-identified, or anonymized? (Y/N) If No: Why?	
Will the PI remain in a raw format (still identifiable)? (Y	

If Yes: why?	
If the PI is being anonymized, aggregated, or de-identifie will that function be performed by VSABC or by our ven	

Data Storage, Residency, & Access	
Where will the data be stored?	
In which country will the data be stored? If outside of Canada, please provide details.	
Who will have access to the data? List all parties (by role accessing PI as part of the regular operational activities o this project.	
How long will the PI be stored? Why is it being stored fo time period specified?	

Compliance Documents	
Is there an agreement in place with the vendor (if applica (Y/N?) If yes, describe the type of agreement (e.g. service contra information-sharing agreement)	
Does the agreement include specific privacy protection clauses? These are separate and apart from “confidentiali clauses.	

H. Information Sharing Agreements (ISAs) and Template

Name of Public Bo	Effective Date of ISA	Expiry Date of ISA	Location of ISA
ICBC	October 6, 2010	April 6, 2015	Director of Finance a Operations
B.C. Ministry of Finance	June 20, 2014	Until revoked	Director of Finance a Operations

INFORMATION SHARING AGREEMENT TEMPLATE

dated the _____ day of _____, 20____

BETWEEN:

[First Party]

("Party X")

Agreement Administrator:

_____

Party X

Ph:

_____

Fax:

_____

Email:

_____

AND:

[Other Party]

("Party Y")

Agreement Administrator:

_____

Party Y

Ph:

Fax:

Email:

Add other parties as required.

1. Purpose

The purpose of this Agreement is to document the terms and conditions of the exchange of certain personal information by the Parties, in compliance with the *Freedom of Information and Protection of Privacy Act* and other applicable legislation (if any).

2. Personal Information

In this Agreement, "Personal Information" means:

Insert description of information to be covered by the Agreement. If different types of information are to be handled differently under the Agreement, break the definition down accordingly.

Collection and Disclosure of Personal Information

Describe the exchange of information under the Agreement. If different types of informat are to be collected and/or disclosed differently, break the description down accordingly. each receiving body that is a public body, state the authority (under sections 26 and 27) collection. For each disclosing body that is a public body, state the authority (under secti 33) for disclosure. If there are other legislative provisions that work together with the *Freedom of Information and Protection of Privacy Act* to provide authority for collection and/or disclosure, state what those provisions are.

4. Use of Personal Information

Describe the use(s) to which each body will put the information, and state the authority (under section 32) for those use(s). If there are other legislative provisions that govern th use of the information, state what those provisions are.

5. Accuracy

Each Party will make every reasonable effort to ensure the Personal Information in its custody is accurate, complete and up-to-date.

6. Security

6.1 Each Party will make reasonable arrangements to maintain the security of the Personal Information in its custody, by protecting it against such risks as unauthorized access, collection, use, disclosure or disposal.

6.2 Each Party will implement this Agreement in conformity with the government's Information Security Policy.

6.3 Each Party will advise the other Party immediately of any circumstances, incidents or events which to its knowledge have jeopardized or may in future jeopardize:

- the privacy of individuals;
- the security of any computer system in its custody that is used to access the Personal Information.

7. Compliance Monitoring and Investigations

7.1 Each party will record and monitor access to the Personal Information in its custody, in order to establish a chain of responsibility, as follows:

Describe compliance monitoring methodology and timetable. Use an appendix to provide more detail, if required. If using an appendix, change "as follows" to "as set out in Appen "A" to this Agreement".

7.2 Each Party will investigate all reported cases of:

- unauthorized access to or modification of the Personal Information in its custody;
- unauthorized use of the Personal Information in its custody;
- unauthorized disclosure of the Personal Information in its custody;
- breaches of privacy or security with respect to the Personal Information in its custody or with respect to any computer system in its custody that is used to access the Personal Information.

7.3 Each Party will report to the other the results of any such investigation and the steps taken to address any remaining issues or concerns about the security of the Personal Information or computer systems, or the privacy of individuals to whom the Personal Information relates.

8. Modification or Termination of Agreement - General

8.1 This Agreement may be modified or terminated at any time by agreement, in writing, of [both/all] parties.

9. Termination for Non-Compliance with Agreement

9.1 This Agreement may be terminated at any time by either Party if the other Party fails to meet its obligations under this Agreement.

If there are more than two parties, revise paragraph 9.1 as required.

10. Term of Agreement

This Agreement will be in force during the period commencing [Date] and ending [Date] unless sooner terminated in accordance with paragraph 8.1 or paragraph 9.1.

11. Appendices

Any appendices to this Agreement are part of the Agreement. If there is a conflict between a provision in an appendix and any provision of this Agreement, the provision in the appendix is inoperative to the extent of the conflict unless it states that it operates despite a conflicting provision of this Agreement.

If appendices are not used, clause 11 can be deleted.

Agreed to on behalf of Party X:

(Authorized representative) Date

Agreed to on behalf of Party Y:

(Authorized representative) Date

I. Website Policy Statement

Protecting Privacy

The VSA is committed to protecting your privacy and personal information. We do this through responsible privacy management. We collect, use, disclose and dispose of personal information in accordance with our privacy management policies and the FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT, the MOTOR DEALER ACT, provisions of the BUSINESS PRACTICES AND CONSUMER PROTECTION ACT and other legislation.

What is personal information?

Personal information is recorded information about an identifiable individual. Personal information can include an individual's name, address, birthdate, email and phone numbers. When we collect personal information, we are to advise you:

- why it is being collected
- our authority to collect it, and
- the contact information of a person in the Authority who can answer questions about our collection of the information.

What is not personal information?

Contact information is not protected under the legislation from collection, use, or disclosure. Contact information is information that allows someone to be identified at their place of work including their name, title, work address, work email and work phone numbers.

Using Personal Information

We use personal information as part of our administration and enforcement of the MOTOR DEALER ACT and certain provisions of the BUSINESS PRACTICES AND CONSUMER PROTECTION ACT and their regulations. We use personal information we collect for the purposes identified to you or a consistent purpose as allowed by the legislation. We directly collect information by various methods including online and paper forms, emails and surveys. We use this information to:

- assess applicants for suitability to be licensed or registered,
- review licensee or registrant conduct,
- investigate complaints and unlicensed activity,
- process and investigate applications to the Motor Dealer Customer Compensation Fund,
- take appropriate administrative action including hearings before the Registrar, and
- undertake studies and surveys.

Retaining Personal Information

The length of time we retain personal information depends on its nature and use. Factors that determine the length of time information is kept include

- continuing and maintaining regulatory and business relationships,
- retaining information necessary for future legal proceedings,
- information required for statistical purposes,
- information required for archival purposes, and
- information required to be retained for any legislated retention requirements.

Disclosing Information

We do not sell personal information that we collect. However, we may need to disclose personal information:

- to a licensee or registrant to investigate a complaint against the licensee or registrant, to ensure fairness in the process,
- to other law enforcement agencies or organizations to complete an investigation or review an application to the Motor Dealer Customer Compensation Fund,
- at hearings before the Registrar of Motor Dealers which by law are open to the public,
- within decisions of the Registrar of Motor Dealers published on the VSA's website, and
- where compelled by law to disclose the information.

Access to Personal Information

You may request access to your personal information under the FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT. Please make a request by

completing this form and send it by email, fax or by regular mail. Contact information is noted below.

Correction of Personal Information

As a public body, the Authority is bound to make every reasonable effort to ensure that your personal information is complete and accurate. If you encounter factually incorrect data in the personal information we have about you, you have the right to request a correction of the data. Please send us a request in writing that includes a clear description of the error, where it appears in the information we have, and the correction you wish to see made. We will respond to your request for correction within 30 business days.

Canadian Anti-Spam Legislation (CASL)

The VSA does not send out electronic commercial messages or marketing materials to solicit business. The VSA is a not-for-profit Society administering legislation on behalf of the B.C. Government. Our external communications are for industry regulation and consumer awareness initiatives and do not constitute electronic commercial messaging.

Visiting the VSA website – Cookies

A cookie is a small file containing certain pieces of information that a website creates when you visit the site. It can track how and when you use a site, which site you visited immediately before, and it can store that information about you. Cookies cannot be used to run programs or deliver viruses to your computer. There are two types of cookies, session cookies and persistent cookies. Our website may use session cookies which are stored in temporary memory and are not retained after you sign out or close the browser session.

For example, we use cookies to support our visitors by helping their browser to remember form selections during a browsing session. Likewise, through the third-party tool and plugin Google Analytics, we can reference anonymous, non-persistent data to understand broad traffic patterns about our visitors allowing us to better refine our site to our client's needs.

Additionally, to protect our visitors, our security platform and web hosting company may alert us to unusual, abusive or actively malicious behavior tied to a specific IP address or region. To safe

guard all visitors, traffic deemed malicious may then be permanently or temporarily blocked from visiting the site.

Web browser information relating to visits to the Authority's website is considered to be a form of personal information. This includes the following:

- The web browser and operating system you are using
- The dates / times of your visit
- The pages or services you accessed on our site
- Your Internet Protocol (IP) network domain name and address of the computer you are using to access our site

Our website does allow users to reject the use of cookies. By doing so, the VSA websites' functionality may be limited.

Other website links

There are links to other websites on the VSA website. The VSA's privacy statement applies only to the VSA website and no other websites.

Who to contact

Privacy Officer
Vehicle Sales Authority of British Columbia
280 – 8029 199th Street, Langley, B.C. V2Y 0E2

privacy@vsabc.ca

If you have further questions about B.C. privacy legislation or concerns about the VSA's privacy management, you can contact the Office of the Information & Privacy Commissioner of British Columbia.

Office of the Information & Privacy Commissioner for BC
P.O. Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4

Toll Free: 1-800-663-7867

Deputy Commissioner: 250-387-5629

info@oipc.bc.ca