Vehicle Sales Authority
of British Columbia

VEHICLE SALES AUTHORITY

PRIVACY POLICIES AND PROCEDURES

Effective November 1, 2014
Ver. 1

Table of Contents

1. Introduction

1.1. Purpose of the Policies and Procedures

The Vehicle Sales Authority ("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 generally 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 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,.

1.2. Important terms

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

BPCPA	means the *Business Practices and Consumer Protection Act* S.B.C. 2004 c. 2
Board Appointee	means a person appointed to the Board of Directors of the VSA but has not as yet attended their first meeting
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 other information that is protected from disclosure by law.
Contact information	has the same meaning as in Schedule 1 of FIPPA, *information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual*

FIPPA	means the *Freedom of Information and Protection of Privacy Act* R.S.B.C. 1996 c. 165
FIPPA-R	the *Freedom of Information and Protection of Privacy Act Regulation* B.C. Reg. 155/2012
License, licensed, and licensing	means for a motor dealer, registration as a motor dealer under the MDA, and for a salesperson, licensed as a salesperson under the *Salesperson Licensing Regulation* B.C. Reg. 241/2004
MDA	means the *Motor Dealer Act* R.S.B.C. 1996 c. 316
MDCCFB	means the Motor Dealer Customer Compensation Fund Board which decides whether or not a consumer who has made a claim will be awarded compensation.
MDCCFB Member	means a person who has been appointed to the Motor Dealer Customer Compensation Fund Board but has not as yet attended their first meeting
OIPC	means Office of the Information and Privacy Commissioner
Personal information	has the same meaning as in Schedule 1 of FIPP, *recorded information about an identifiable individual other than contact information*
PIA	means 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

1.3. 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 market place.
8. Advise to the B.C. government on any aspect of the motor vehicle sales market place.

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* R.S.B.C. 1996 c. 238.

1.4. VSA Logo Official Marks

The following are the registered Official Marks of the Motor Dealer Council of British Columbia, doing business as the Vehicle Sales Authority of British Columbia (the "VSA"), and may not be used or reproduced in whole or in part, in any colour or font and in any combination or individually:

(a) by motor dealers or salespersons unless directed to by the Registrar in accordance with the *Motor Dealer Act*, or

(b) by any other person unless they receive prior written approval from the VSA.

"Vehicle Sales Authority of British Columbia"

"Vehicle Sales Authority"

"VSA"

1.5. 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 enquiry@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 0E2

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.
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 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 MDCCFB. [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 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 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 persons 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 ss. 33 to 36 of FIPPA [s. 27(1)(a)(iii) and (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 which includes investigations under the MDA [s. 27(1)(c)(iv) - FIPPA]
(e) Necessary to manage or decide to terminate an employee of the VSA [s. 27(1)(f) - FIPPA]
(f) 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 Enquiry and Complaint Handling Policy
(b) Inspection, Liaison Visits, Investigations and Progressive Enforcement Policy
(c) Dealer and Salesperson Licensing Policy
(d) Hearing Policy, and
(e) Motor Dealer Customer Compensation Fund Board Claim Processing and Adjudication policy.

4.7.2 The above policies are to be available to the public on the VSA's 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(b) – 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]

6.1. How a request must be made

6.1.1. A person may request access to information held by the VSA.

6.1.2. A request under paragraph 6.1.1 is to 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. 33.1(1)(b) – 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 brother or sister 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 consider if notice to the Minister responsible for FIPPA must be provided [s. 30.2 – 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 is possible. It is incumbent on the privacy officer to ensure coverage while they are on vacation.

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 A letter acknowledging that the request has been received is to be sent to the applicant that notes:

(a) the date the request was received;

(b) that the VSA has 30 business days to respond to the request and provide the date;
(c) that the 30 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;
(d) if the applicant would accept electronic disclosure via a password protected CD-ROM; and
(e) who the requesting person may contact regarding their access request.

6.4.3 All correspondence should be in writing and a copy of all correspondence and notes are to be placed in the electronic and/or hard copy file.

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 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 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. To ensure consistency and thoroughness in searching for information, the VSA uses an information/record search form found in **Appendix D** to assist in identifying where records may be located.

6.6.2. The privacy officer must search for electronic and hard copy versions of information in the filing room and the VSA's database system.

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

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

6.6.5 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.

6.7. 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 To ensure clarity and consistency in assessing fees, the privacy officer is to use the Fee Estimate Form found in **Appendix E** [Schedule 1 of FIPPA-R].

6.7.3 An estimate is to be provided as soon as is possible, and should be provided no later than 14 days after receipt of the request, unless circumstances require more time.

6.7.4 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.

Where the request involves a mix of personal information of the requester and non-personal information, a fee can be charged for producing the non-personal information. [s. 75(2) – FIPPA]

6.7.5 A business may request access to records in order 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 a 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 severe 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. and the Ministry of Finance if their information is potentially to be disclosed [s. 12 – 22, 25, 35, and 36 – 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. The original hard copy file is to be copied and left unmarked and unaltered.

6.9.6. Where an entire document or page of a document is to be withheld, the privacy officer must complete the Refusal of Disclosure Form found in **Appendix F**. The Refusal of Disclosure Form is put in the same place as the document or page that is removed and not disclosed.

6.9.7. 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.

6.9.8. Once the records have been reviewed and redacted, the privacy officer is to attach a Disclosure Summary Form such as found in **Appendix G**.

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.

(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 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 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.

[s. 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
(b) Registrar's hearing decisions
(c) Summary of Motor Dealer Customer Compensation Fund Board decisions
(d) Undertakings by licensee's
(e) 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
(f) 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
(g) Information on unlicensed activity
(h) Educational material for consumers and industry members
(i) Application materials,
(j) Fee schedules, and
(k) 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 it cannot be corrected.

8.2.3 When incorrect factual information was used to make a decision directly affecting an individual and the corrected factual information could have influenced the outcome of the decision, the VSA may review that decision, subject to applicable legal principles.

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 the 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.

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.

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 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 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 [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 *Document Disposal Act* and its Records Retention Protocol.

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 H**.

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) Security policies;
(c) Human resources security;
(d) Technical 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 follows the procedures found 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 that 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 following steps are used to address privacy breaches. As the circumstances for each privacy breach vary, these steps might occur concurrently or in quick succession; they do not necessarily follow the order given below:

(a) **Report Immediately**

(i) Employees must report suspected or actual privacy breaches immediately to the Privacy Officer. The Privacy Officer is to report immediately to the Office of the Privacy Commissioner when needed.

(ii) In all cases, the person who identifies a breach must make the call themselves if they are not able to reach the Privacy Officer.

(b) **Contain the Privacy Breach**

(i) The VSA should take immediate action to contain the privacy breach and to limit its impact. Appropriate actions will depend on the nature of the breach and may include:

- Isolating or suspending the activity that led to the privacy breach;
- Correcting all weaknesses in physical security;
- Taking immediate steps to recover the personal information, records or equipment from all sources, where possible; and
- Determining if any copies have been made of personal information that was breached and recovering where possible.

(ii) If the breach includes the loss of electronic equipment, contact the IT department to see if the equipment can be remotely wiped.

(c) **Access the Extent and Impact of the Privacy Breach**

(i) As part of the Investigation, the VSA will work with others to determine the:

1) Personal Information Involved;
2) Cause and Extent of the Breach;
3) Individuals Affected by the Breach; and
4) Foreseeable Harm from the Breach;

(d) **Contact IT** to see if a mobile device, such as an iPad or iPhone, that has been lost or stolen can be tracked or remotely wiped of data to protect the information it contains.

(e) **Document the Privacy Breach and Corrective Action Taken**

(i) As part of the Investigation, the VSA will work with others to:

1) Ensure that evidence of the privacy breach is preserved; and
2) Document the privacy breach in detail.

(f) **Consider Notifying Affected Individuals**

(i) The impact of privacy breaches must be reviewed to determine if it is appropriate to notify individuals whose personal information has been affected

by the breach. As part of the Investigation, the privacy officer will notify affected parties and take other required actions, as appropriate.

(g) **Inform Other Parties as Appropriate**

(i) As part of the investigation, the privacy officer will notify the affected parties and take other required actions, as appropriate. Affected parties may include, for example: insurers, professional or other regulatory bodies, third-party contractors, internal business units, or unions.

(ii) The privacy officer is solely responsible for liaising with the OIPC regarding an actual or suggested privacy breach. The following factors are relevant in determining whether to report a privacy breach to the OIPC:

1) The sensitivity of personal information;
2) Whether the breached information could result in identity theft or other harm, including pain and suffering of loss of reputation;
3) A large number of people are affected by the breach;
4) The information has not been fully recovered; and
5) The breach is the result of a systemic problem or a similar breach has occurred before.

(h) **Prevent Future Privacy Breaches**

(iii) The VSA will work with others to investigate and manage the privacy breach.

(iv) The VSA will, as applicable, implement recommendations resulting from an investigation.

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 which 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 require the VSA 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 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.

12.1.3 The Privacy Impact Assessment directions can be found in **Appendix I**.

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.

12.4. Directions on Conducting a PIA

12.4.1. Terms used in this section:

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 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 means the linking or combining of Personal Information in one database with Personal Information in one or more other databases if the purpose of the linking or combining is different from:

(a) The purpose for which the information in each database was originally obtained or compiled; and
(b) Every purpose that is consistent with each purpose referred to in paragraph (a).

Data-Linking Initiative means a new or newly revised system, project, program or activity that has, as a component, Data Linking between:
(a) Two or more Public Bodies; or
(b) One or more Public Bodies and one or more agencies.

Personal Information Bank (PIB) means a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Privacy Risk means something that could cause the unauthorized access, collection, use, disclosure, or storage of Personal Information.

12.4.2. The VSA is directed to include the following elements, where applicable, in any PIA conducted:

(a) A detailed description of the system, project, program or activity covered by the PIA;
(b) A list of the elements of information including Personal Information included in the system, project, program or activity;
(c) Identification of any information including Personal Information involved in the system, project, program or activity that can be assessed from and/or stored outside Canada;
(d) Identification of whether the system, project, program or activity involves Data Linking;
(e) Identification of whether the system project, program or activity involves a Common or Integrated Program or Activity;
(f) An information flow diagram and/or Personal Information flow table that shows how the system, project, program or activity does, or will, collect, use, and/or disclose Personal Information. Information, including the authorities for the collection, use, and disclosure of Personal Information under FIPPA;
    (i) an information flow diagram must be included if the system, project, program or activity is related to a Common or Integrated Program or Activity or a Data-Linking Initiative;
(g) Identification of the Privacy Risks within the system, project, program or activity and for each Privacy Risk identified:
    (i) an explanation of the likelihood of the Privacy Risk occurring;
    (ii) an explanation of the degree of impact the Privacy Risk would have on an individual if it occurred; and
    (iii) a record of the mitigations that have been, or will be, implemented;

(h) A description of the physical security measures related to the system, project, program or activity;
(i) A description of the technical security measures related to the system, project, program or activity;
(j) A description of any specific policies and procedures within the VSA governing an Employee's management of Personal Information;
(k) With respect to technical systems, details of access to Personal Information including as applicable, but not limited to:
    (i) a description of the permissions governing access to the Personal Information;
    (ii) a description of how access to Personal Information is, or will be, tracked; and
    (iii) a description of any access controls and/or ways in which unauthorized changes to Personal Information is, or will be, limited or restricted;
(l) An explanation of how the accuracy of an individual's Personal Information is, or will be, ensured;
(m) An explanation of how an individual's Personal Information is, or will be, corrected upon their request or an explanation of how an individual's Personal Information is, or will be, annotated if it is not corrected as per the individual's request;
(n) With respect to Personal Information, an explanation of the retention and disposition measures that relate to the secure retention and disposition of Personal Information;
(o) With respect to Personal Information that is used to make a decision that directly affects an individual, an explanation of how any applicable retention and disposition requirements are, or will be, met;
(p) An explanation of any systematic disclosures or regular exchanges of Personal Information included in the system, project, program or activity and reference to any applicable ISA(s);
(q) For research that is not out of scope of FIPPA [s. 3(1)(e) – FIPPA], identification of whether the system, project, program or activity does, or will, involve access to Personal Information for research or statistical purposes and reference to the research agreement, as required [s. 35(1)(d) – FIPPA] ; and
(r) Identification of whether the system, project, program or activity does, or will, involve a PIB and, where applicable, the PIB summary information for inclusion in a public directory [s. 69(6) – FIPPA].

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. See **Appendix J**.

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) documents 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 term of the agreement.

The provisions of FIPPA that authorize the collection, use of 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 to 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, who will represent the MDCCF and keep the minutes and provide administrative support
3. One representative from the following departments chosen by each department annually:

    (a) Administrative
    (b) Finance
    (c) Compliance and Investigations
    (d) Licensing
    (e) Learning
    (f) Consumer Services; and
    (g) Communications

4. The President of the VSA.

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

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

1) Review of the current policies and procedures as needed
2) Roundtable discussion on privacy and privacy security issues at the VSA and at the MDCCF

3) Discussion on a privacy topic selected by the Committee at its prior meeting. Each member will take turns leading the discussion
4) Education on FIPPA to be led by the Privacy Officer or another committee member
5) 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 found in **Appendix K**.

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, 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 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 *Document Disposal Act* which 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].

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:**

internally and externally?	Compliance, Licensing, Administration and Christina for advertising concerns. **Externally:** Dealers, consumers, complainants/complainant representatives.
When sharing information, do we share personal information such as an individual's address, telephone number or bank information?	**Internally:** Generally all information is shared without redaction. **Externally:** Certain personal information is redacted when information is shared externally (ex. 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 otherwise 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) and (i); 26, 27, 33.1(i.1); (l), 33.1(2); 33.2(a), (c), (d), (i), and (l) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32 *Motor Dealer Act Regulation* sections: 7, 13, *Salesperson Licensing Regulation* sections: 4, 8. *Business Practices and Consumer Protection Act* sections: 149 and 150. Restrictions on disclosure in the *Motor Dealer Act*: section 29(1)

COMPLIANCE AND 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	▪ Dealer's name, registration number, address(s) ▪ Offer to Purchase identifying make, model or car being purchased/trade-

collects from motor dealers or other businesses and organizations we interact with.	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?	**<u>Internally:</u>** Consumer services, Licensing, Administration and management as needed. **<u>Externally:</u>** ▪ Dealers, salespeople, by-law, CVSE, ICBC, CRA, CBSA, and financial institutions as needed ▪ Policy 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. **<u>Legislative Authority:</u>** FIPPA sections: 22(4)(c) and (i); 26, 27, 33.1(i.1); (l), 33.1(2); 33.2(a), (c), (d), (i), and (l) *Motor Dealer Act* sections: 4, 7, 12, 25, 26, 32, *Motor Dealer Act Regulation* sections: 7, 13, *Salesperson Licensing Regulation* sections: 4, 8. *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) and (i); 26, 27, 33.1(i.1); (l), 33.1(2); 33.2(a), (c), (d), (i), and (l)

	Motor Dealer Act sections: 4 and 7 *Salesperson Licensing Regulation* Sections: 4 and 8 Restriction 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 (witnesses).	**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). ▪ 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 information sharing agreement)?	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: 22(4)(c) and (i); 26, 27, 33.1(i.1); (l), 33.1(2); 33.2(a), (c), (d), (i), and (l) *Motor Dealer Act* sections: 4 and 7 *Salesperson Licensing Regulation* sections: Sections 4 and 8 Restriction 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?	**Internally:** Learning, Consumer Services and Compliance. **Externally:** ▪ 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) and (i); 26, 27 33.1(i.1); (l), 33.1(2); 33.2(a), (c), (d), (i), and (l) *Motor Dealer Act* sections:

	4, 7, 12, 25, 26, 32, *Motor Dealer Act Regulation* sections: 7, 13, *Salesperson Licensing Regulation* sections: 4, 8. *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: "Securit" 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 the individual's consent or otherwise rely on legislative authority (an information sharing agreement)?	Have consent when processing personal information (processing of credit card payments, refunds, etc.). **Legislative Authority:** FIPPA sections: 33.1(i.1), and 33.2(a)

B. Privacy Access Request Form

BRITISH COLUMBIA
The Best Place on Earth

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

ARCS NO.
292-30/
292-40/

REQUEST FOR ACCESS TO RECORDS

NAME OF PUBLIC BODY TO WHICH YOU ARE DIRECTING YOUR REQUEST

YOUR NAME			
LAST NAME	FIRST NAME	MIDDLE NAME	MISS MS MRS. MR. OTHER : _____

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

YOUR CONTACT INFORMATION		
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 ONLY

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

Vehicle Sales Authority
of British Columbia

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 R.S.B.C. 1996 c.165

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

the 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

Signature: _____

Name: _____
first name *last name*

Witness

Signature: _____

Name: _____
first name *last name*

Occupation: _____

D. Information/Record Search Form

Vehicle Sales Authority
of British Columbia

INFORMATION SEARCH FORM

Freedom of Information and Protection of Privacy Act **R.S.B.C. 1996 c. 165**

(Form last updated November 1, 2014)

Access to information request of: _____.

Access Request File #: _____.

Person(s) conducting search for information: _____.

Search start date: _____, 20___. Search end date: _____, 20___.

Total Time spent (hours and/or minutes) _____.

Guidelines for Conducting Information Searches

1. The scope of the search is determined by the request for information. Obtain clear instructions from the Privacy Officer.
2. Review one file/computer/database at a time until completed.
3. Information may be in any form such as paper, electronic, post-it notes, scratch paper etc.
4. Look for "linked" files such as an enquiry file that has become an investigation file.

Summary of Documents Located:

This summary will assist in estimating any fees to be charged for the production of documents, therefore accuracy is important:

1. There are ____ pages of 8.5" x 11" or 14" records located in hard copy form. N/A ☐.
2. There are ____pages of "oversized" (11" x 17") records located in hard copy form. N/A ☐.
3. There are (approximately) _____ pages of records located in electronic form. N/A ☐.
4. There are _____ photographs located. N/A ☐.
5. Data is believed to exist in a currently inaccessible database: Yes ☐ No ☐ N/A ☐.
6. There are ___video cassettes ___audio cassettes ___DVDs and/or ___CDs located. N/A ☐.

Search for Records/Information in Hard Copy Form:

	Records Located			Comments
	Yes	No	N/A	
Motor Dealer File #_____	☐	☐	☐	_____
Salesperson File # _____	☐	☐	☐	_____
Investigation File # _____	☐	☐	☐	_____
Case File # _____	☐	☐	☐	_____
Complaint File # _____	☐	☐	☐	_____
Compensation Fund File # _____	☐	☐	☐	_____
Financial Information _____	☐	☐	☐	_____
Policy & Procedures _____	☐	☐	☐	_____
Communications _____	☐	☐	☐	_____
Learning Division _____	☐	☐	☐	_____
Other _____	☐	☐	☐	_____
Other _____	☐	☐	☐	_____
Other _____	☐	☐	☐	_____

Additional Comments:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Search for Records/Information in Electronic Form:

	Records Located			Comments
	Yes	No	N/A	
Motor Dealer File #_____	☐	☐	☐	_____
Salesperson File # _____	☐	☐	☐	_____
Investigation File # _____	☐	☐	☐	_____
Case File # _____	☐	☐	☐	_____
Complaint/Enquiry File # _____	☐	☐	☐	_____
Compensation Fund File # _____	☐	☐	☐	_____
Financial information _____	☐	☐	☐	_____
Policy & Procedures _____	☐	☐	☐	_____
Communications _____	☐	☐	☐	_____
Learning Division _____	☐	☐	☐	_____
Emails _____	☐	☐	☐	_____
Global Capture Report _____	☐	☐	☐	_____
Other _____	☐	☐	☐	_____
Were there attachments/uploads included with any electronic files?	☐	☐	☐	_____

Additional Comments:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Additional Searches

	Records Located			Comments
	Yes	No	N/A	
Was the Compliance Officer(s) for the region/complaint asked for any additional records?	☐	☐	☐	If Yes, name(s) _____ _____ _____
Was the Compliance Officer's computer and H: drive reviewed for information?	☐	☐	☐	_____
Was the Licensing Officer(s) for the region/complaint asked for any additional records?	☐	☐	☐	If Yes, name(s)_____ _____ _____
Was the Licensing Officer's computer and H: drive searched for information?	☐	☐	☐	_____
The computer and H: drive of _____ was searched for information.	☐	☐	☐	_____
The computer and H: drive of _____ was searched for information.	☐	☐	☐	_____
The computer and H: drive of _____ was searched for information.	☐	☐	☐	_____

Additional Comments:

_____
_____
_____
_____
_____
_____
_____

_____

E. Fee Estimate Form

Vehicle Sales Authority
of British Columbia

FEE ESTIMATE FORM
***Freedom of Information and Protection of Privacy Act* R.S.B.C. 1996 c. 165**
***Freedom of Information and Protection of Privacy Regulation* B.C. Reg. 323/93**

A review of your requested information indicates that there are approximately _____ pages for review and copying. Your request is not solely for personal information of _____ (requesting party), but also information relating to others. In accordance with section 75(1) of the *Freedom of Information and Protection of Privacy Act* (the **"**FIPPA"), the *Freedom of Information and Protection of Privacy Regulation* B.C. Reg. 323/93 (the "Regulation") and *Re*: *Inquiry Regarding British Columbia Securities Commission Records* Order 00-19 (decision of the Privacy Commissioner), the VSA may charge a fee for certain services and copies of documents. We provide you with an estimate of those fees we require you to pay: **[Add or remove items as needed as set out under s. 7 of the Regulation]**

Item	Description	Estimated	Estimated Fee	Legislative Authority
1.	Locating and accessing records (first 3 hours free)			s. 75(1) of FIPPA s. 7(1)(a) of the Regulation
2.	For preparing a record for disclosure and handling a record (collating, stapling, organizing)			s. 75(1) of FIPPA s. 7(1)(d) of the Regulation
3.	Photocopies and computer printouts (8.5" x 11" or 14").			s. 75(1) of FIPPA s. 7(1)(f)(i) of the Regulation
4.	For Commercial Applicants (delete items 1 to 3 and charge the actual cost of producing the documents)			s. 75(1) of FIPPA s. 7(2) of the Regulation
	Estimated Total			

The above is an estimate only and the actual amount of the fees may be more or less than estimated.

In considering that the Vehicle Sales Authority (the "VSA") is a not-for-profit society exercising delegated authority, the VSA requires you to pay a deposit of $_____before any review is commenced per: Sub-section 75(4) of FIPPA. You may ask that the above fees be waived or reduced under Subsection 75(5) of FIPPA by making a written request to the Privacy Officer. Under Sub-section 7(4) of FIPPA, the time in which the VSA must respond to your access request does not begin to run until:

(a) the head of the public body [Privacy Officer] excuses the applicant from paying all of the fees under section 75 (5);

(b) the head of the public body [Privacy Officer] excuses the applicant from paying part of the fees under section 75 (5), and the applicant agrees to pay the remainder and, if required by the head of a public body[Privacy Officer], pays the deposit required;

(c) the applicant agrees to pay the fees set out in the written estimate and, if required by the head of a public body [Privacy Officer], pays the deposit required.

Please write to us and let us know if:

(a) you accept our fee estimate and will pay the requested fees; or
(b) you are seeking a fee reduction and/or waiver and your reason for asking for a reduction and/or waiver.

If you agree to pay our fees and a deposit has been requested, please also include payment of the deposit in your correspondence.

Dated: _____, 20___.

_____

Ian Christman Privacy Officer

(Form last updated November 1, 2014)

F. Refusal of Disclosure Form

Vehicle Sales Authority
of British Columbia

DISCLOSURE REFUSAL
***Freedom of Information and Protection of Privacy Act* R.S.B.C. 1996 c. 165**
***Freedom of Information and Protection of Privacy Regulation* B.C. Reg. 323/93**

Description:

{Description}

Reason(s) for Refusal:

{Sections of FIPPA} {Reasons}

Date Reviewed:

Reviewed by:

_____

Ian Christman
Privacy Officer
Deputy Registrar/Director of Licensing

(Form last updated November 1, 2014)

G. Disclosure Summary Form

Vehicle Sales Authority
of British Columbia

RECORDS DISCLOSURE SUMMARY

***Freedom of Information and Protection of Privacy Act* R.S.B.C. 1996 c. 165**
***Freedom of Information and Protection of Privacy Regulation* B.C. Reg. 323/93**

Description:

{Description}: {number} ({number}) pages from the hard copy file and 78 pages from the electronic database.

Redactions/ Refusals of Disclosure:

A. Redactions.

None

B. Refusals of Disclosure

None

Date Reviewed:

Reviewed by:

_____

Ian Christman
Privacy Officer

(Form last updated November 1, 2014)

H. Procedures for Removing Records from the Office

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

PROTECTING PERSONAL INFORMATION OUTSIDE THE OFFICE

(Replaces: Guidelines for Protecting Personal Information When Travelling on Business)

February 2005

Whether you're travelling with personal information or working with it at home or another location, personal information can more easily be lost or compromised when it's outside your office. Common sense measures can and should be taken to reduce risks to personal information in such situations.

Private sector organizations covered by the *Personal Information Protection Act* (PIPA) and public bodies covered by the *Freedom of Information and Protection of Privacy Act* (FOIPPA) must take reasonable measures to protect personal information from risks such as unauthorized collection, use or disclosure and are legally liable if they fail to do so. This document offers tips on some steps that can be taken to protect personal information when you take it outside the office and tips on protecting personal information when you're working with it at home.

The following tips apply to "personal information", which is "information about an identifiable individual". The word "organization" is used below to refer to both organizations under PIPA and public bodies under FOIPPA

This document has benefited from a similar publication of the Office of the Information and Privacy Commissioner for Ontario.

Please read the important notice at the end of this document about the nature and status of this document.

WORKING WITH PERSONAL INFORMATION OUTSIDE THE OFFICE

Never travel with personal information unless you absolutely must have it with you. If you take personal information with you, take the least amount that you need and leave the rest behind. If possible, you should only take copies, leaving original documents in the office.

While away from your office or your home, laptops and other electronic devices containing personal information (including PDAs such as Palm Pilots and Blackberrys) should be kept with you. If you must leave a laptop or other device somewhere, make sure it is in a location secure from theft, loss and unauthorized

access to personal information. (See below for more.)

Laptops and other electronic devices such as PDAs should be password protected.

Access to personal information should be password protected, including when stored on a password-protected storage device such as a floppy disk, CD or USB storage drive, rather than the hard drive of your laptop or home computer.

Electronic records of sensitive personal information when taken away from the office should be encrypted.

While away from your office or your home, storage devices containing copies of personal information should be kept in a locked briefcase or other container that is kept with you. If you must leave a storage device somewhere, do so in a location secure from theft, loss and unauthorized access to personal information.

When working outside the office, log off or shut down your laptop or home computer when you're not using it. Set the automatic logoff to run after a short period of idleness.

When working outside the office, protect your laptop by using locks and alarms as appropriate. As best you can, you should always keep control of your laptop. If this is not possible, you should store your laptop in a secure location such as a locked room or desk drawer.

Do not share a laptop used for working with private information with other individuals, including family members and friends.

If the records you need are too voluminous to carry with you, send them to your destination by a trustworthy courier.

You should avoid viewing personal information in public, including while travelling on airplanes, trains, buses and public transit. Do so only if you absolutely must and take precautions to ensure no one else can view the personal information. For example, your laptop screen should not be viewable by fellow passengers. Set your laptop's screensaver to run after one minute of idleness. Also consider installing a privacy screen filter on your laptop screen, to hinder viewing of the screen from an angle.

When in transit or working outside the office, avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard and can be intercepted.

You should avoid discussing personal information in public, including busses, commuter trains, subways, airplanes, restaurants or on the street. If you must do so, ensure others cannot overhear.

When travelling or working outside your office you should keep personal information under your control, including during meals and other breaks. If this is not possible, store the personal information in a secure location, such as a locked room or desk drawer. Do not leave personal information in plain view or unattended in an insecure place, such as an unlocked office or meeting room.

Do not leave records containing personal information in plain view in your hotel room. Consider storing the records at a local office of your organization overnight. If your hotel room or hotel office has a safe, store the personal information there.

Records containing personal information have gone missing over the years when locked vehicles have been broken into or the vehicle has been stolen. Although the trunk of a vehicle is generally considered more secure than the interior of a vehicle, records have been stolen from locked trunks, so extreme caution must be exercised. Records should only be left in a vehicle if there is no other option. They should be locked in the trunk, not left in plain view in the vehicle interior. They also should be left only if the vehicle is parked in a secure location and then only for brief periods. If a staff person must travel regularly with personal information, a car alarm should be installed to enhance the security of records while in transit.

When working at home, you should store personal information in a locked filing cabinet or desk drawer when not being used. The filing cabinet or desk should only contain work-related records and no one else should have access to it.

You should avoid storing personal information on the hard drive of your home computer. Any personal information that is stored on hard drives should be encrypted and password protected. You should ensure your home computer has effective Internet security measures such as anti-virus software and firewalls.

If you telecommute from home, your employer should provide you with a separate phone line and password-controlled voice-mail box.

You should avoid sending personal information by email or fax from public locations, including Internet cafes. If it is absolutely necessary to do so, see the tips on email and faxing in other OIPC website resources.

You should fax or photocopy personal information yourself when working outside the office. If you have to ask someone else to do this for you, you should be present.

Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely. Any working notes you created during the trip that contain personal information should also be stored in a secure environment as soon as possible.

If personal information is stolen or lost, immediately notify your supervisor and the person responsible for privacy compliance in your organization, 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

Other resources are available to help you meet your obligations regarding working with personal information away from your office, including the following:

Office of the Information and Privacy Commissioner/Ontario, *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office*: http://www.ipc.on.ca/images/Resources/wrkout-e.pdf

M 224

BRITISH COLUMBIA

PRIVACY IMPACT ASSESSMENT DIRECTIONS

TO:	**HEADS OF PUBLIC BODIES THAT ARE NOT GOVERNMENT MINISTRIES**
DIRECTION:	2/14
SUBJECT:	Directions to heads of Public Bodies that are not government ministries on conducting 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 Public Bodies that are not government ministries.
EFFECTIVE DATE:	May 9, 2014

Andrew Wilkinson.

Honourable Andrew Wilkinson
Minister of Technology, Innovation and Citizens' Services

Minister of Technology, Innovation and Citizens' Services

Directions to Heads of Public Bodies that are not Government Ministries issued under Section 69 (5.3) of the Freedom of Information and Protection of Privacy Act

I, Andrew Wilkinson, Minister of Technology, Innovation and Citizens' Services, issue the following directions to heads of Public Bodies that are not government ministries under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996 c. 165:

A. Definitions

For the purposes of these directions:

"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" means the linking or combining of Personal Information in one database with Personal Information in one or more other databases if the purpose of the linking or combining is different from

a. the purpose for which the information in each database was originally obtained or compiled, and

b. every purpose that is consistent with each purpose referred to in paragraph a.

"Data-Linking Initiative" means a new or newly revised system, project, program or activity that has, as a component, Data Linking between

a. two or more Public Bodies, or

b. one or more Public Bodies and one or more agencies.

"Employee", in relation to a Public Body, includes**:**

a. a volunteer, and

b. a service provider.

"Information Sharing Agreement (ISA)" means an agreement between a public body and one or more of the following:

a. another Public Body;
b. a government institution subject to the *Privacy Act* (Canada);
c. an organization subject to the *Personal Information Protection Act* or the *Personal Information Protection and Electronic Documents Act* (Canada);
d. a public body, government institution or institution as defined in applicable provincial legislation having the same effect as this Act;
e. a person or a group of persons;
f. a prescribed entity

that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.

"Personal Information" means recorded information about an identifiable individual other than contact information.

"Personal Information Bank (PIB)" means a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

"Privacy Impact Assessment (PIA)" means an assessment that is conducted by a Public Body to determine if a current or proposed system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act*.

"Privacy Risk" means something that could cause the unauthorized access, collection, use, disclosure, or storage of Personal Information.

"Public Body" means

a. a ministry of the government of British Columbia,

b. an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2 of the *Freedom of Information and Protection of Privacy Act*, or

c. a local public body but does not include

d. the office of a person who is a member or officer of the Legislative

Assembly, or e. the Court of Appeal, Supreme Court or Provincial Court

B. General Directions

Under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, heads of
Public Bodies that are not government ministries are directed to:

1. conduct any PIA in accordance with sections B and C of these directions;

2. ensure that a PIA is signed by individuals with primary responsibility for privacy and, where relevant, security.

C. Directions on Conducting a PIA

Under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, heads of Public Bodies that are not government ministries are directed to include the following elements, where applicable, in any PIA conducted:

1. a detailed description of the system, project, program or activity covered by the PIA;

2. a list of the elements of information including Personal Information included in the system, project, program or activity;

3. identification of any information including Personal Information involved in the system, project, program or activity that can be accessed from and/or stored outside Canada;

4. identification of whether the system, project, program or activity involves Data Linking;

5. identification of whether the system, project, program or activity involves a Common or
Integrated Program or
Activity;

6. an information flow diagram and/or Personal Information flow table that shows how the system, project, program or activity does, or will, collect, use, and/or disclose Personal
Information, including the authorities for the collection, use, and disclosure of Personal
Information under the Freedom of Information and Protection of Privacy Act;

   i. an information flow diagram must be included if the system, project, program or activity is related to a Common or Integrated Program or Activity or a Data- Linking Initiative;

7. identification of the Privacy Risks within the system, project, program or activity and for each Privacy Risk identified:

i. an explanation of the likelihood of the Privacy Risk occurring;

ii. an explanation of the degree of impact the Privacy Risk would have on an individual if it occurred; and

iii. a record of the mitigations that have been, or will be, implemented;

8. a description of the physical security measures related to the system, project, program or activity;

9. a description of the technical security measures related to the system, project, program or activity;

10. a description of any specific policies and procedures within the Public Body governing an Employee's management of Personal Information;

11. with respect to technical systems, details of access to Personal Information including as applicable, but not limited to:

i. a description of the permissions governing access to the Personal Information;

ii. a description of how access to Personal Information is, or will be, tracked; and

iii. a description of any access controls and/or ways in which unauthorized changes to Personal Information is, or will be, limited or restricted;

12. an explanation of how the accuracy of an individual's Personal Information is, or will be, ensured;

13. an explanation of how an individual's Personal Information is, or will be, corrected upon their request or an explanation of how an individual's Personal Information is, or will be, annotated if it is not corrected as per the individual's request;

14. with respect to Personal Information, an explanation of the retention and disposition measures that relate to the secure retention and disposition of Personal Information;

15. with respect to Personal Information that is used to make a decision that directly affects an individual, an explanation of how any applicable retention and disposition requirements are, or will be, met;

16. an explanation of any systematic disclosures or regular exchanges of Personal Information included in the system, project, program or activity and reference to any applicable ISA(s);

17. for research that is not out of scope of the *Freedom of Information and Protection of Privacy Act*, as per section 3 (1) (e) of that Act, identification of whether the system,

project, program or activity does, or will, involve access to Personal Information for research or statistical purposes and reference to the research agreement, as required under section 35 (1) (d) of the *Freedom of Information and Protection of Privacy Act*; and

18. identification of whether the system, project, program or activity does, or will, involve a PIB and, where applicable, the PIB summary information required under section 69 (6) of the *Freedom of Information and Protection of Privacy Act* for inclusion in a public directory.

J. Information Sharing Agreements (ISAs) and Template

Name of Public Body	Effective Date of ISA	Expiry Date of ISA	Location of ISA
ICBC	October 6, 2010	April 6, 2015	Director of Finance and Operations
B.C. Ministry of Finance	June 20, 2014	Until revoked	Director of Finance and 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 information are to be collected and/or disclosed differently, break the description down accordingly. For each receiving body that is a public body, state the authority (under sections 26 and 27) for collection. For each disclosing body that is a public body, state the authority (under section 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

the 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 Appendix "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

K. Audit Checklist

Office of the
Information & Privacy
Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

Securing Personal Information: A Self-Assessment Tool for Organizations

March, 2012

How well is your organization protecting personal information? The personal information security requirements under the *Personal Information Protection Act (British Columbia), Personal Information Protection Act (Alberta)* and the *Personal Information Protection and Electronic Documents Act [PIPEDA] (Canada)* require organizations to take reasonable steps to safeguard the personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The first step in developing reasonable safeguards is to collect only the personal information that is needed for a particular purpose. If it is not needed, organizations should not collect it. But if they do, they need to take appropriate precautions.

Reasonable safeguards include several layers of security, including, but not limited to:

- risk management,
- security policies,
- human resources security,
- physical security,
- technical security,
- incident management, and
- business continuity planning.

The reasonableness of security arrangements adopted by an organization must be evaluated in light of a number of factors including:

- the sensitivity of the personal information,
- the foreseeable risks,
- the likelihood of damage occurring,
- the medium and format of the record containing the personal information,
- the potential harm that could be caused by an incident, and
- the cost of preventive measures.

Generally accepted or common practices in a particular sector or kind of activity may be relevant to the reasonableness of a security safeguard. However, generally accepted practices and technical standards must be complemented by elementary caution and common sense.
In creating this tool, we reviewed other standards (such as those produced by the ISO) and received feedback from various organizations in Alberta, British Columbia, and Atlantic Canada.

Questions in blue indicate the minimum security requirements for any organization, regardless of its size or the sensitivity of the personal information it holds. The remaining questions help organizations raise their security standards beyond those minimum levels.
The goal is to be able to answer “yes” to each question.

Blue text indicates a minimum security requirement.

CONTENTS

Risk Management

1.1 Has the organization identified what personal information assets are being held, and their sensitivity?

1.2 Has the organization analyzed, evaluated and documented: The business impacts that might result from personal information security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the information?

1.3 Has the organization analyzed, evaluated and documented: The personal impacts on customers and employees?

1.4 Has the organization analyzed, evaluated and documented: The likelihood of security failures occurring, considering possible threats and vulnerabilities?

1.5 Has the organization analyzed, evaluated and documented: The estimated levels of residual risks?

1.6 Has the organization analyzed, evaluated and documented: Which risks are acceptable?

1.7 Has management formally approved the risk identification in writing?

Risk Treatment

1.8 Does a risk treatment plan identify the appropriate management action, resources, responsibilities and priorities for managing personal information security risks?

Risk Reviews

Are risk assessments conducted at planned intervals to review the residual risks and the identified acceptable levels of risks, taking into account changes to:.

1.9 The organization?

1.10 Technology?

1.11 Business objectives and processes?

1.12 Identified threats?

1.13 Possible future threats?

1.14 External events, such as changes to the legal or regulatory environment, contractual obligations and social climate?

1.15 When the organization identifies changes to risks, is the focus and/ or priority placed on the most significantly changed risks and their associated preventive action requirements?

1.16 Are threat and risk assessments (TRAs) scheduled annually?

1.17 Is there a process trigger for when a non-scheduled TRA or Privacy Impact Assessment (PIA) is required (e.g. security or privacy incident, new threats)?

Policies

2.1 Do operational security policies exist? (For example, policies around secure faxing of personal information, policies and procedures for end-of-day closing, policies for using couriers to send personal information and/or policies for reviewing audit logs.)

2.2 Have the operational security policies been endorsed by management?

2.3 Has the responsibility for reviewing and updating the organization's policies, procedures, guidelines and standards been defined and assigned?

2.4 Is the personal information security policy reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness?

2.5 Are independent reviews of the security policies carried out on a regular basis to ensure compliance with current legislative standards?

2.6 Are organizational policies and standards updated as a result of this review?

2.7 Can the security officer responsible for the policy update the policy and republish it to the organization?

2.8 Do employees, contractors and partners have easy access to the personal information security policy?

2.9 Do customers have access to information about the organization's personal information security policy?

2.10 Do incentives exist for employees, contractors, customers and partners to understand and follow the policy?

2.11 Does the organization track acceptance and measure awareness of security policies?

2.12 Is there a policy for hardware maintenance and upgrades?

2.13 Is there a network security infrastructure policy that includes a copy of a current network diagram?

2.14 Does the network security policy require that system security documentation be protected from unauthorized access?

2.15 Is there a policy controlling or prohibiting hardware and software not purchased or supported by the organization and their use on the network?

2.16 If personal information is collected over the Internet, is there a specific policy to manage this practice?

2.17 Is there a policy that governs access to personal information and

IT assets, networks and systems from outside the organization (e.g. remote working, teleworking)?

2.18 Is there a policy concerning travelling with personal information?

2.19 Is there an acceptable use policy?

2.20 Are there policies and appropriate security controls in place governing electronic mail, instant messaging, social networks, blogs, and so on?

Records Management

Information Classification

3.1 Is there an information classification policy?

3.2 Does the information classification policy clearly outline how personal information is to be handled and protected?

3.3 Have an appropriate set of procedures for information labelling and handling been developed and implemented to support the information classification scheme adopted by the organization?

3.4 Are users informed of any applicable privacy legislation and repercussions of improper classification?

Retention of personal information

3.5 Have specific retention periods been defined for all personal information (and in accordance with various legal, regulatory or business requirements)?

Destruction of personal information

3.6 Is personal information contained on obsolete electronic equipment or other assets securely destroyed before the equipment or asset is disposed of? For example, are the internal hard drives of faxes and printers properly disposed of when replacing old equipment?

3.7 Are hard copy records containing personal information shredded, mulched or otherwise securely destroyed?

3.8 Is personal information on magnetic media destroyed by overwriting, degaussing or using some other approved method?

3.9 Are the contents of erasable storage media containing personal information obscured using an appropriate technique before the medium is reused?

Human Resources Security

Executive Leadership

4.1 Does management actively support personal information security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of

personal information security responsibilities?

4.2 Is there a management-level employee (and management-level contractor representative, where a contract is in place) identified as responsible for security practices?

4.3 Is there a functional forum of management representatives from IT and business units to coordinate and implement personal information security controls?

Training

Has training been implemented for all employees, data custodians and management to ensure they are aware of and understand:

4.4 Their security responsibilities?

4.5 Security policies and practices?

4.6 Permitted access, use and disclosure of personal information?

4.7 Retention and disposal policies?

4.8 Requirements for password maintenance and proper password security?

4.9 Is annual privacy and security training a requirement for any handling of personal information?

4.10 Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training?

4.11 Are there consequences for compromising keys, passwords and other security policy violations?

4.12 Is completion of privacy and security training tracked?

Confidentiality Agreements

4.13 Are employees required to sign confidentiality agreements?

4.14 Do the agreements clearly define individual responsibilities for security, including the protection of personal information?

4.15 Is responsibility for security an integral part of an individual's annual performance objectives?

4.16 Is individual performance with respect to security and confidentiality routinely reviewed (i.e., annually) with the individual by management?

Hiring and Terminations

4.17 Are potential employees who will have access to personal information adequately and appropriately screened?

4.18 Is there a process to ensure immediate recovery of keys and pass cards, and the revocation of access privileges and appropriate notification of security personnel when a termination (voluntary or

involuntary) occurs?

Contractors and Third Parties

4.19 Are private sector organizations and individuals who have access to personal information adequately and appropriately screened?

4.20 Are the necessary security requirements specified in any contractual documentation?

4.21 Do all contracts that involve personal information contain a privacy protection schedule?

4.22 Are contractors required to comply with the organization's privacy and security policies or equivalent policies to ensure that contractors are bound by the same legislated privacy standards as the organization?

4.23 Are security controls in place to govern the activities of contractors, customers and partners who may have access to the organization's systems and data?

4.24 Does a knowledgeable employee supervise external hardware or software maintenance personnel whenever maintenance is undertaken?

4.25 Are contractors and other third parties required to return personal information to the contracting organization upon completion of the contract?

4.26 If not required to return the information, are contractors and other third parties required to securely destroy, using an approved method, the information at the completion of the contract?

4.27 Are there regular inspections and/or audits (scheduled and unscheduled) of contractors and third parties to ensure compliance with security and privacy standards?

4.28 Are there contractual provisions in place to control outsourcing of any role involving personal information to sub-contractors?

Physical Security

Do physical security measures used for storing personal information include:

5.1 Locked cabinets?

5.2 Locked office doors?

5.3 Pass cards?

5.4 Motion detectors and other intrusion alarm systems?

Is there a secure area for servers containing personal information ensuring:

5.5 Walls extend from the floor to ceiling?

5.6 Physical access is restricted to authorized personnel?

5.7 Accesses to the secure space are logged and routinely reviewed?

5.8 Visitors are escorted by an authorized individual while in the secure space?

5.9 Motion detectors and alarms are used?

5.10 If any personal information is stored on local hard drives, is that equipment bolted to the floor?

5.11 Are publicly accessible service counters kept clear of personal information?

Is there a nightly closing protocol requiring employees to:

5.12 Clear all personal information from desks and place files containing personal information in locked filing cabinets?

5.13 Lock all office doors and cabinets?

5.14 Log out of all computers?

5.15 Remove all documents containing personal information from fax machines and printers?

5.16 Set intrusion alarms (where installed)?

5.17 Are access points such as delivery and loading areas and other points where unauthorized persons may enter the premises controlled and, if possible, isolated from information processing facilities to avoid unauthorized access?

Systems Security

Terminals and Personal Computers

6.1 Are terminals and personal computers used for handling personal information positioned so that unauthorized personnel cannot see their screens?

6.2 Are terminals and personal computers used for handling personal information positioned so that they are not readily visible from outside the facility?

6.3 If a user walks away from his or her terminal, is there an automatic process to lock out all users after a defined period of inactivity (e.g. screensaver requiring the authorized user to log on again)?

Mobile and Portable Devices

6.4 Is there a policy governing the use of mobile devices and removable media if personal information is stored on them?

6.5 Is the policy reviewed and updated on a regular basis?

6.6 Does the policy require that the least amount of personal information be stored on the device?

6.7 Is personal information encrypted when stored on mobile and

portable devices, as well as on removable media?

6.8 Is personal information deleted from mobile and portable devices as soon as possible?

6.9 Are there reasonable controls in place to prevent the theft of mobile computing and portable devices when left unattended?

6.10 Are controls in place to prevent or restrict the connection of personal mobile devices (e.g. iPods) or removable media (e.g. USB drives) to the organization's networks and systems?

6.11 Where mobile or portable devices are allowed to connect to the organization's networks or systems, are they checked to ensure that appropriate security controls (e.g. firewall, anti-virus software) are installed and correctly configured?

6.12 Are removable media used to store personal information stored in secure containers when not in use? (e.g. locked in a secure cabinet)

6.13 Are laptops containing personal information cable-locked to desks when in use or otherwise equipped with an alarm that will sound if an attempt is made to remove the laptop?

Systems Security (cont.)

If equipment such as a laptop computer is removed from the premises on a temporary basis by staff, are control procedures in place to:

6.14 Record the identity of the user?

6.15 Confirm the authority of the user to access the personal information on the equipment?

6.16 Record the return of the equipment?

6.17 Is laptop encryption prevented from being disabled by the user?

6.18 Are laptops equipped with a tracking device, a remote kill-switch, and/ or remote deletion of data?

6.19 Are laptops configured so that users are prevented from changing security settings or downloading other software onto the laptop?

Network Security

Network security includes the system of computers, routers, cables, switches and wireless access points. It is the entire system of transport and storage technologies.

7.1 Are networks segregated physically and/or logically to separate systems containing personal information from public networks such as the Internet?

7.2 Where a local area network containing personal information is connected to a public network, does the organization use perimeter

defence safeguards (e.g. firewalls, routers, intrusion detection or prevention systems, anti-virus/anti-spyware software, etc.) to mediate all traffic and to protect systems that are accessible from the Internet?

7.3 Are systems that are exposed to the Internet (e.g. web servers and their software) or servers supporting sensitive applications "hardened" (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication)?

7.4 Are ports closed or Internet connections disabled on computers where services are not needed?

7.5 Are these safeguards regularly updated?

7.6 Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?

7.7 Are SSL (Secure Socket Layer) or other secure connection technologies (e.g. virtual private network (VPN)) used when receiving or sending personal information?

Wireless

WARNING:. We believe that, at this time, there are significant security risks to any handling of personal information using wireless networks. You should therefore carefully consider whether you should use wireless technology to handle personal information. If you do accept the risks, ensure your wireless technology is as secure as possible.

8.1 Is there a policy in place that addresses the use of wireless technology?

8.2 Does the organization ensure that wireless networks are not used until they comply with the organization's security policy?

8.3 Are users on the network aware of the risks associated with wireless technology?

8.4 Does the organization have a complete and current inventory of all wireless devices?

8.5 Does the organization perform comprehensive security assessments at regular and random intervals (including identifying, locating and removing unauthorized wireless access points and other devices)?

8.6 Has the organization completed a site survey to measure and establish the wireless coverage for the organization?

8.7 Are access points located in such a way as to minimize the risk of unauthorized physical access and manipulation?

8.8 Are access points located in the interior of the organization's premises instead of near external walls and windows?

8.9 Are default parameters on wireless devices (e.g. passwords, identification codes) changed?

8.10 Are the strongest available security features of the wireless devices, including encryption and authentication, enabled?

8.11 Are additional safeguards (e.g. firewalls, anti-virus, etc.) installed on all wireless devices?

8.12 Are wireless capabilities (e.g. wireless cards in laptops) disabled (either permanently or when not required)?

8.13 Are unnecessary services (e.g. file sharing) disabled?

8.14 Is a wireless intrusion detection and prevention capability deployed on the network to detect suspicious behaviour or unauthorized access and activity?

8.15 Are audit records of security- and privacy-relevant activities on the wireless network created and reviewed on a regular basis?

Database Security

9.1 Is a data dictionary (table of contents) used to document, standardize and control the naming and use of data?

9.2 Is access to the data dictionary restricted and monitored?

9.3 Are database maintenance utilities that bypass controls restricted and monitored?

9.4 If there is a software failure, is the system capable of automatically recovering the database?

9.5 Have automated or manual controls been implemented to protect against unauthorized disclosure of personal information?

9.6 Are methods in place to check and maintain the integrity of the data (e.g. consistency checks, checksums)?

9.7 Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?

9.8 Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information?

9.9 Are default parameters on the database (e.g. accounts, passwords, etc.) changed?

9.10 Is there a formal approval process in place for handling requests for disclosure of database contents or for database access, and does this process include steps to evaluate privacy impacts and security risks?

Operating Systems

An operating system is the core software on the computer that allows the operation of all of the other software. The most common operating systems are Microsoft Windows, Mac OSX, Unix and Linux.

10.1 Are operating systems kept up-to-date with all patches and fixes?

10.2 Is there a regular schedule for updating definitions and running scans with anti-virus, anti-spyware and anti-rootkit software?

10.3 Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?

10.4 Are all network services (e.g. websites or e-mail servers) running on computers connected to the network documented and authorized?

10.5 Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information?

10.6 Is accurate time and date information maintained on computers to track malicious usage or errors appropriately?

E-mail and Fax Security

11.1 An organization should consider whether it is appropriate to transmit personal information by e-mail or fax. If it decides to do so, is a policy in place that addresses the use of fax and e-mail transmission of personal information?

11.2 Are regularly updated lists of fax numbers, e-mail addresses and other contact information produced and distributed to ensure that employees use current and accurate contact information?

When faxing personal information, are the following steps taken:

11.3 The receiver is notified in advance of the fax?

11.4 The receiver stands by to receive the data or the receiver confirms that their fax machine is in a secure location?

11.5 The sender takes the utmost care to ensure the accuracy of the fax number dialled?

11.6 A fax cover sheet is always used and always includes the name, address and phone number of both the sender and receiver?

11.7 The transmission is encrypted?

11.8 A confidentiality notice is attached?

11.9 Are pre-programmed fax numbers regularly checked to ensure accuracy?

11.10 Are fax machines used to send or receive personal information positioned in a secure area?

11.11 Is access to fax machines used to send and receive personal information controlled using access keys and passwords?

11.12 Are fax activity history reports retained to check for unauthorized transmissions?

11.13 Are the internal hard drives of faxes and printers properly disposed of when replacing old equipment?

11.14 Are fax confirmation reports carefully checked to ensure the correct transmission of personal information?

11.15 Are fax machines used for the transmission and receipt of personal information only used by authorized staff?

11.16 When sending e-mail messages to more than one recipient, is the bcc field used?

Data Integrity and Protection

This section is intended to be specific to securing the data from unauthorized modification.

12.1 Is there a procedure in place to ensure that any removal of personal information from the premises has been properly authorized?

12.2 Is there an archiving process that ensures the secure storage of data, and guarantees the continued confidentiality, integrity and availability of the data?

12.3 Are encryption and other secure mechanisms in place for both the transport and storage of personal information?

12.4 Are automated or manual controls, or both, used to prevent unauthorized copying, transmission, or printing of personal information?

12.5 Are there policies and procedures in place to protect against unauthorized modification of data?

12.6 When transmitting personal information where data integrity is a concern, is an integrity mechanism used to verify that the data has not been altered during transmission (e.g. digital signatures)?

12.7 Is there a process to revert and resolve changes if the data-integrity verification process fails?

12.8 Are data and software integrity tools (such as Tripwire) used to detect unexpected changes to files?

Access Control

General

13.1 Is there an access control policy? For example, are there policies requiring username and password when you log in? Are there policies governing access to the operating system and each database?

13.2 Does the network access policy include a requirement that each user, at login, is informed of the date and time of the last valid logon and any subsequent failed logon attempts?

13.3 Are controls in place to detect any discrepancies in logon attempts?

User Registration, Access and Approval

13.4 Is a formal user registration process in place?

13.5 Does the user registration process include: verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not granted until formally approved?

13.6 Is each user of a system that processes personal information uniquely identified?

13.7 When assigning a unique identifier for users, does the organization ensure the proper identification of the individual to whom the identifier is being issued, before giving the user access to the system?

13.8 Is the identification of the authorizer retained in the transaction record?

13.9 Is a current, accurate inventory of computer accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts?

13.10 Is there a formal process to assign defined roles to users?

13.11 Does the access control policy clearly state the information access privileges for each defined role in the organization?

13.12 Does the role assignment process contain steps to ensure personal information is withheld from unauthorized individuals (e.g. manufacturers, maintenance staff)?

13.13 Is a data custodian role defined that includes access control, data integrity, as well as backup and recovery?

13.14 Has the role been defined for maintaining the access control lists?

13.15 Are roles and access rights for partners and third-party organizations (such as consultants, off-site storage) clearly defined?

13.16 Are privileges allocated on a need-to-use basis, and allocated, modified or changed only after formal authorization?

13.17 Are access privileges limited to the least amount of personal information required to carry out job-related functions?

13.18 Is there a clearly defined separation or segregation of duties (e.g. someone who initiates an event cannot authorize it; roles cannot overlap)?

13.19 Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals?

Authentication

13.20 Where a system user is authenticated, is the authentication information, such as password, not displayed, and is it protected from unauthorized access?

Where user identification and authentication mechanisms are used to protect personal information, are procedures implemented that:

13.21 Control the issue, change, cancellation and audit of user identifiers and authentication mechanisms?

13.22 Ensure that authentication codes or passwords are generated, Controlled and distributed so as to maintain the confidentiality and availability of the authentication code?

13.23 Are the authentication mechanisms that are implemented commensurate with the sensitivity of the information and the associated risks (i.e. the more sensitive the information, the more robust the authentication mechanisms. For example, is two-factor authentication used when handling sensitive personal information, including financial information)?

13.24 Where authentication is based on username and password, are effective password policies in place?

Are passwords:

13.25 Known only to the authorized user of the account?

13.26 Pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition?

13.27 No less than eight characters in length?

13.28 One-way encrypted?

13.29 Excluded from unprotected, automatic logon processes?

13.30 Changed at least semi-annually?

13.31 Changed at frequent and irregular intervals?

Information Systems Acquisition, Development and Maintenance

Hardware

14.1 Are security requirements identified as part of any new system development, acquisition or enhancement?

14.2 Does the organization have a configuration-management or change control process (e.g. source code control, tickets and resolutions)?

Software

14.3 Are privacy and security considered in the process of obtaining new third-party software?

14.4 Is there a patch management process for new security vulnerabilities?

14.5 Is there a separate environment for development and testing?

14.6 Do the development and testing environments contain test data only? Test data should not be drawn from current or past real data.

14.7 Are development personnel restricted from having access to the production environment?

14.8 Is there a policy that prohibits the use of unauthorized software?

14.9 Are there controls that prevent or detect unauthorized software?

Maintenance

14.10 Are systems containing personal information maintained only by appropriately screened personnel?

Incident Management

15.1 I s there a privacy incident management policy in place? Has the organization appointed an individual or established a centre to coordinate incident response?

15.2 Is there a privacy incident management policy in place? Do these procedures include guidance for the exchange of incident-related Information with designated individuals and organizations in a timely fashion?

Does the privacy incident management policy include:

15.3 Incident detection and analysis

15.4 Containment, mitigation and recovery strategies

15.5 Notification and reporting requirements

15.6 Post-incident analysis (“lessons learned”)

15.7 Prevention strategies

15.8 Are the individuals assigned to incident response roles adequately trained?

15.9 Are the incident response procedures practised and tested on a regular basis?

15.10 Does the organization use a variety of mechanisms (e.g. firewalls, routers, intrusion detection and prevention systems, audit logs, system performance tools, etc.) to continuously monitor the operations of their systems to detect anomalies in service delivery levels?

Does the organization maintain records that show how incidents were handled, including:

15.11 Documenting the chain of events during the incident, noting the date and time when the incident was detected?

15.12 The actions taken?

15.13 The rationale for decisions made?

15.14 Details of any communications?

15.15 Management approvals or direction?

15.16 Any external and internal reports?

Does the organization perform a post-incident analysis that summarizes the cause and impact of the incident, including costs, and identifies:

15.17 Security deficiencies?

15.18 Measures to prevent a similar incident (e.g. modifications to existing safeguards or the addition of new safeguards)?

15.19 Measures to reduce the impact of a recurrence?

15.20 Improvements to incident response procedures?

Business Continuity Planning

Organizations need to ensure that they can continue to operate in the event of an interruption to their operations (e.g. IT system failures, supply chain problems, natural disasters).

16.1 Is there a process in place to develop and maintain business continuity throughout the organization?

16.2 Has the organization conducted an impact analysis to identify and prioritize the organization's critical services and assets?

Does the business continuity plan address:

16.3 Different levels of interruption of service?

16.4 Physical damage?

16.5 Environmental damage?

16.6 Unauthorized modification or disclosure of information?

16.7 Loss of control of system integrity?

16.8 Physical theft?

16.9 Has the organization made provisions for the continuous review, testing and audit of business continuity plans?

16.10 Has the business continuity plan been subject to appropriate departmental or regulatory expert review (e.g. legal, policy, finance, communications, information management and human resource specialists)?

16.11 Are backup processes in place to protect essential business information such as production servers, critical network components, configuration backup, etc?

16.12 Are backups stored off site?

16.13 Are remote backups and recovery procedures tested at regular intervals?

16.14 Where 100% availability is essential, are duplicate databases maintained on separate physical devices and are all transactions performed simultaneously on both databases?

16.15 Have all databases and data repositories been identified?

16.16 Are mechanisms in place to monitor the organization's level of overall readiness?

Compliance

Audit Process Design

17.1 Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?

17.2 Are all system/audit logs that relate to the handling of personal information: Securely and remotely logged to a read-only medium that has an alert system when tampering is attempted?

17.3 Are all system/audit logs that relate to the handling of personal information: Regularly monitored?

Ongoing Audits

17.4 Are procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly?

17.5 Are proactive audits conducted at regular intervals to verify the logical and physical consistency of the data, in order to identify discrepancies such as lost records, open chains, incomplete sets and improper usage?

17.6 Is active monitoring in place to ensure that personal information cannot be passed between computers, or between discrete systems within the same computer, without authority?

Scheduled Audits

17.7 Is software/hardware inventory maintained in an up-to-date fashion?

17.8 Is an annual physical inventory of all storage media containing personal information performed and are discrepancies investigated immediately and corrected?

Audit Verification

17.9 Are audit monitoring and review procedures in place to promptly detect errors in procedures and results?

Audit Implementation

17.10 Do the management personnel responsible for the audited area oversee the implementation of audit recommendations, verify completion of implementation and report verification results?

Offi ce of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4
Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca