BC ASSESSMENT

BOARD POLICY
Personal Information Protection Policy BP 03-0162

1. Purpose and Scope

This policy describes the principles and practices that the British Columbia Assessment Authority ("BCA") follows to protect personal information.

The policy also applies to any service providers that collect, use or disclose personal information on behalf of BCA.

This policy has been developed and adopted in compliance with the requirements of British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA).

2. Background

FIPPA sets out the ground rules for how public sector bodies covered by FIPPA may collect, use and disclose personal information.

In order to carry out its legislated mandate, BCA collects customer information, some of which may be personal information, as follows:

(a) BCA collects, uses and discloses information from questionnaires submitted by property owners and third parties (including the Land Title and Survey Authority and local governments) respecting the assessment of land and improvements under the authorities set out in the *Assessment Act*. Information on BCA's public website is published in accordance with the *Assessment Act* and FIPPA. Because BCA has the statutory authority to publish an assessment roll accessible through the BC Online information service, some personal information is available through that service.

(b) BCA collects and uses information provided by customers as part of their registration procedures for a BCA customer account. The registration procedure for a BCA customer account includes acknowledgement of consent to the collection of this information and a proviso that such information will be collected, used and disclosed in accordance with FIPPA.

When required to do so, BCA informs customers and other individuals of the reasons why their personal information is being collected, and how it will be used and disclosed.

3. References

This policy statement is consistent with the following:

- *Freedom of Information and Protection of Privacy Act*

- *Assessment Act*
- *Assessment Act Regulation 433/98*
- *Assessment Authority Act*
- Assessment Authority Act Regulations – 497/77
- Mandate Letter with Province
- BCA Website Statements:
  - Terms of Use
  - Privacy Statements
  - BCA Website: Privacy Management and Accountability Program

4. Definitions

***Contact information*:** Information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or FIPPA.

***Customer*:** For the purposes of this policy, includes persons who own, occupy or dispose of property under the *Assessment Act* and/or have a BCA Customer Account.

***BCA Customer Portal*:** BCA's electronic customer portal which provides a single point of entry for customers (including members of the public) to access BCA's online digital products, services and information (including BCA's assessment search website).

***Manager, Information Access & Privacy*:** The BCA employee designated by the President & CEO to support BCA's compliance with and to carry out the duties and responsibilities of BCA as a public body under FIPPA.

***Personal Information*:** Recorded information about an identifiable individual other than contact information (described above).

5. Collecting Personal Information

To fulfill BCA's mandate to establish and maintain property assessments and provide customers access to BCA's customer portal and public website, BCA collects information, some of which may be personal information, from its customers that is necessary to:

- complete a new assessment roll;
- deliver a notice of assessment and other products to each person named in the assessment roll;
- provide electronic access to products and services;
- ensure a high standard of products and services to customers;
- enable communication with customers;
- meet statutory and regulatory requirements; and

- process payments for BCA's services.

6. Using and Disclosing Personal Information

(a) BCA uses and discloses personal information collected from customers for the purposes of operating British Columbia's property assessment systems and processing requests from customers, or to carry on other necessary or advisable activities related to fulfilling our statutory obligations, including:

- when BCA requires legal advice from a lawyer;
- for the purposes of collecting a debt;
- to protect BCA and customers from fraud; and
- to investigate an anticipated breach of an agreement or a contravention of law.

(b) The *Assessment Act* section 8 requires that BCA make the assessment roll available for public inspection during regular business hours of each BCA area office. The roll may be searched and inspected by any person, subject to certain criteria. A property owner's contact information may be accessible through such a search, but cannot be used to conduct a search.

(c) Long standing approaches to search functionality, and those in place for personal information that is publicly available, restrict customer search services [for example, each search must proceed individually (no ability to search in bulk)]; the criteria to conduct an individual search is limited to folio ID (area, jurisdiction, roll number), parcel identifier number, plan number, and civic address, upon agreement with BCA's of terms of use. Property owner name and mailing address is available for the current roll year only.

(d) When so requested, property owners are advised how to seek protection of privacy in assessment rolls and records [in accordance with *Assessment Act* section 68(1)].

(e) BCA uses and discloses its property owners' and customers' personal information in accordance with applicable laws, including the *Assessment Act* and FIPPA for purposes relating to producing the assessment roll and records and related purposes, and carrying out other necessary and advisable activities related to producing the assessment roll.

(f) BCA does not sell or provide lists of its customers' personal information to other parties who do not have the statutory authority to obtain that information.

7. Retaining Personal Information

(a) If BCA uses an individual's personal information to make a decision that directly affects the individual, that personal information is retained for at least one year so that the individual has a reasonable opportunity to request access to it.

(b) Subject to 7(a), an individual's personal information is retained as necessary to fulfill the identified purposes or a legal or business purpose, as determined by BCA in accordance with its legislation, and record and retention policies and procedure.

8. Ensuring Accuracy of Personal Information

(a) Reasonable efforts are made to ensure that an individual's personal information is accurate and complete where it may be used to make a decision about the individual or be disclosed to another person or organization.

(b) An individual may request a correction to his/her personal information in order to ensure its accuracy and completeness.

(c) If the personal information which is the subject of a correction request is demonstrated to be inaccurate or incomplete, BCA will correct the information as required and send the corrected information to any organization to which the personal information has been disclosed in the previous year. ("Disclosed" as used in this context does not include where another organization has obtained such personal information by conducting a search of the assessment roll or records operated by BCA.) If the requested correction is not made, the correction request will be noted in the file.

9. Securing Personal Information

(a) BCA is committed to ensuring the security of personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

(b) The following measures are in place to ensure personal information security:

- Operational BCA records are stored securely with direct physical access to the records limited only to BCA employees and eligible external parties who have been accredited with direct access privileges based upon need-to-know and least privilege.
- External parties who are accredited with direct access privileges (for example, by virtue of statutory authority) to BCA's operational records are limited to accessing that information based upon their statutory authority. They are not permitted to perform "bulk searches" or "sift through" operational records other than that required to fulfill their statutory obligations.
- BCA uses state-of-the art data security and disaster recovery standards and technology which are characteristic of mission-critical computer systems. Personal information is protected in accordance with BCA's Privacy Statements and Terms of Use, along with the following BCA policies:
    - Information Management Policy
    - Information Security Policy
    - IT Asset Disposal Procedures
    - IT Incident Reporting and Handling Procedure
- Appropriate security measures are followed when destroying customers' personal information.
- BCA requires that third-party service providers that will deal in any way with personal information in the possession of BCA to enter into contracts whereby

the third-party service providers agree to manage all BCA information in compliance with FIPPA. Use of the BCA's General Service Agreement, including Schedule E – Privacy Protection, will meet this requirement.

- Personal information is stored on secure servers and employees are not permitted to transfer this information to any other storage media, including removable devices (for example, USB drives), unless such storage has been approved and documented by the employee's manager based on a clear business need and the device is encrypted in accordance with the Information Security Guidelines for Employees policy. Once the storage is no longer needed, copies must be deleted and data must be removed from the storage media or the storage media must be destroyed in a manner that will not allow the content to be recovered.

(c) In the event of a privacy breach:

- An employee, officer or director of BCA, or an employee or associate of a service provider to BCA, must take immediate steps to notify the Manager, Information Access & Privacy of any known or suspected privacy breach (as defined in Appendix 1: Privacy Breach Protocol). BCA responds and manages privacy breaches in accordance with FIPPA and the guidelines set out in Appendix 1: Privacy Breach Protocol.

10. Public Complaints

BCA addresses and manages privacy complaints in accordance with FIPPA and the guidelines set out in Appendix 2: Privacy Complaint Protocol.

11. Privacy Contact

BCA's Manager, Information Access & Privacy is the designated contact person for all inquiries relating to BCA's compliance with the requirements of FIPPA.

Inquiries should be forwarded in writing to:

Manager, Information Access & Privacy
BC Assessment
400 – 3450 Uptown Blvd.
Victoria, BC V8Z 0B9

Phone: 1.866.825.8322
Email: access&privacy@bcassessment.ca

APPENDIX 1: PRIVACY BREACH PROTOCOL

A **privacy breach** includes the loss of, unauthorized access to, or unauthorized collection, use, disclosure, or disposal of personal information. Security breaches that do not involve personal information are not privacy breaches. All security breaches must be resolved in accordance with the Information Security Incident Management Policy.

A privacy breach can arise from a number of events and may be accidental or deliberate, including:

- loss or theft of personal information;
- loss or theft of a mobile device;
- transfer of personal information to those which are not entitled to receive the relevant information;
- unauthorized access to a system or to personal information and/or storage of that personal information;
- changes to personal information;
- unauthorized use of a system for the processing or storage of personal information.

BC Assessment (BCA) is a public body under FIPPA and, as such, is required to protect the personal information in our custody or under our control as set out in section 30 of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

> Section 30 of FIPPA states:
>
> *A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

Accountable privacy management[1] includes program controls to ensure that FIPPA's requirements in respect of personal information protection are met. One such program control is a privacy breach protocol.

This protocol outlines the steps BCA takes to manage known or suspected privacy breaches and is based on the Office of the Information and Privacy Commissioner's privacy breach management guidelines[2]. The Manager, Information Access & Privacy is responsible for the coordination, investigation and resolution of privacy breaches under this protocol.

Report, Contain, Recover, Document

A privacy breach should immediately be reported to BCA's Manager, Information Access & Privacy. The Manager, Information Access & Privacy will take immediate steps to contain the privacy breach, including seeking assistance from employees identified by the Manager,

[1] *Accountable Privacy Management in BC's Public Sector* (https://www.oipc.bc.ca/guidance-documents/1545)

[2] *Privacy Breaches: Tools and Resources* (https://www.oipc.bc.ca/guidance-documents/1428)

Information Access & Privacy (or designated employees). Designated employees will cooperate and assist as directed by the Manager, Information Access & Privacy, including to:

- stop unauthorized practice;
- recover records;
- shut down the system that was breached;[3]
- revoke or change computer access codes;
- correct physical security weaknesses.

The Manager, Information Access & Privacy will keep the Executive apprised of any privacy breaches and their management.

The Manager, Information Access & Privacy will liaise with the Office of the Information and Privacy Commissioner (OIPC), President & Chief Executive Officer, and the General Counsel & Corporate Secretary with respect to any recommended public comments regarding a privacy breach.

The Manager, Information Access & Privacy or designate will document the privacy breach and the steps of the privacy breach management process as they occur, including:

- number of affected individuals;
- type of personal information involved;
- possible uses of the personal information, including exploitation, fraud or other harmful uses;
- who is in receipt of the personal information;
- cause and extent of breach;
- containment efforts;
- risk evaluation;
- notification;
- preservation of evidence of the privacy breach;
- prevention strategies and security safeguards.

See Appendix A1: Privacy Breach Checklist.

Risk Evaluation

The Manager, Information Access & Privacy or designate will, within two business days of discovering the privacy breach, conduct a risk evaluation to determine whether affected individuals should be notified. The Manager, Information Access & Privacy will consult with the General Counsel & Corporate Secretary about the outcome of the risk evaluation and the need

[3] If the system involves access to statutory services, including BC Online, the relevant Director will provide direction.

for notification.

Evaluating the risks includes considering the personal information involved, the number of affected individuals, the cause and extent of the privacy breach, and the foreseeable harm from the privacy breach[4]. Foreseeable harm includes harm to individuals or BCA as a result of the privacy breach.

Affected individuals must be notified if the privacy breach could reasonably be expected to cause them significant harm. In assessing whether the privacy breach could cause significant harm, consider risks relating to:

- personal safety;
- identity theft;
- fraud;
- access to assets;
- financial loss;
- loss of business or employment opportunities;
- a breach of contractual obligations;
- hurt, humiliation, embarrassment and damage to reputation or relationships.

In assessing harm to BCA, consider if the privacy breach could result in risks relating to:

- loss of public trust and confidence;
- loss of assets;
- financial exposure;
- loss of contracts or business;
- public safety;
- breach of contractual obligations.

If the data was encrypted, the potential harm may be reduced and notification may not be required. Password protection is not encryption.

The Information and Privacy Commissioner must be notified if the privacy breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals.

The risk evaluation process, including decisions regarding whether or not to notify, should be documented. See Appendix 1A: Privacy Breach Checklist.

Notification

If notification is to occur, it should occur as soon as possible after discovering the privacy

[4] See Step 2: Evaluate the risks in the OIPC's *Privacy Breaches: Tools and Resources* for further information on risk evaluations.

breach and ideally no later than one week thereafter unless notification should be delayed in order to not impede a criminal investigation.

The Manager, Information Access & Privacy or designated employee(s) should notify affected individuals directly (by phone, by letter or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.

Notification of affected individuals should include:

- date of the privacy breach;
- description of the privacy breach;
- description of the personal information involved;
- risk(s) to the individual;
- steps taken to control or reduce the harm;
- future steps planned to prevent further privacy breaches;
- steps the individual can take to control or reduce the harm;
- contact information for the Manager, Information Access & Privacy;
- contact information for the Information and Privacy Commissioner.

As noted above, the Information and Privacy Commissioner must be notified if the privacy breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals.

Assess Security Safeguards and Prevention Strategies

The Manager, Information Access & Privacy or designated employees will assess whether BCA's security safeguards (administrative, physical and technical) are reasonable in light of section 30 of FIPPA.

The Manager, Information Access & Privacy or designated employees will determine whether any improvements or changes to security safeguards are needed as a result of the privacy breach, including determining whether additional preventative measures are necessary. For example:

- audit of physical or technical security;
- root cause analysis;
- revisiting or developing internal policies and procedures;
- additional training.

APPENDIX 1A: PRIVACY BREACH CHECKLIST

Date of report: [Month XX, 20XX]

A. Risk Evaluation

Incident Description

1. Describe the nature of the breach and its cause

2. Date of incident

3. Date incident discovered

4. Location of incident

5. Estimated number of individuals affected

6. Type of individuals affected

B. Personal Information Involved

7. Describe the personal information involved

C. Safeguards

8. Describe physical security measures (locks, alarm systems, etc.)

9. Describe technical security measures

a) Encryption

b) Password

c) Other (Describe)

d) Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual provisions)

D. Harm from the Breach

10. Identify the type of harm(s) that may result from the breach

To individuals (describe for each of the elements below)

a) Personal safety

b) Identity theft

c) Fraud

d) Access to assets

e) Financial loss

f) Loss of business or employment opportunities

g) Breach of contractual obligations

h) Hurt, humiliation, embarrassment and damage to reputation or relationships

i) Other (specify)

To BCA (describe for each of the elementsbelow):

j) Loss of public trust and confidence

k) Loss of assets

l) Financial exposure

m) Loss of contracts or business

o) Public safety

p) Breach of contractual obligations

q) Other (specify)

E. Notification

11. Date and time the Manager, Information Access & Privacy was notified

12. Have the police or other authorities been notified (e.g. professional bodies or persons required under contract) and if “yes”, who was notified and when?

a) If “no”, will they be notified and when?

13. Have affected individuals been notified?

a) If “yes” describe manner of notification

b) Number of individuals notified

c) Date of notification

d) If “no” describe why not?

14. What information was included in the notification? (describe for each of the elements below)

a) Date of the privacy breach

b) Description of the privacy breach

c) Description of the personal information involved

d) Risk(s) to the individual

e) Steps taken to control or reduce the harm

f) Future steps planned to prevent further privacy breaches

g) Steps the individual can take to control or reduce the harm

h) Contact information for the Manager, Information Access & Privacy

i) Contact information for the Information and Privacy Commissioner

15. Should the Office of the Information and Privacy Commissioner be notified of the Breach?

If the privacy breach could reasonably be expected to cause harm to an individual (see factors above) and/or involves a large number of individuals, the Office of the Information and Privacy Commissioner must be notified:

Consider notification if:

a) The personal information involved is sensitive

b) The information has not been fully recovered

c) The breach is the result of a systemic problem or a similar breach has occurred before

d) BCA requires assistance in responding to the privacy breach

e) BCA wants to ensure that the steps taken comply with obligations under privacy legislation

F. Prevention

16. Describe the immediate steps taken to contain and reduce the harm of the breach (e.g. locks changed, computer access codes changed or revoked, computer systems shut down)

17. Describe the long-term strategies you will take to correct the situation (e.g. employees training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security)

If BCA has completed a security audit and is reporting this breach to Office of the Information and Privacy Commissioner, forward a copy of the audit with BCA's report.

APPENDIX 2: PRIVACY COMPLAINT PROTOCOL

A **privacy complaint means** any complaint relating to BCA's compliance with FIPPA, including in relation to the collection, use and disclosure of an individual's personal information or a request for records in the custody or under the control of BCA.

Privacy complaints should be directed to BCA's Manager, Information Access & Privacy by email or in writing to:

Manager, Information Access & Privacy
BC Assessment
400 – 3450 Uptown Blvd.
Victoria, BC V8Z 0B9
Phone: 1.866.825.8322
Email: access&privacy@bcassessment.ca

BCA will consider privacy complaints and respond in writing to the complainant as soon as practical, depending on the nature and extent of the privacy complaint.

All BCA employees must cooperate in a timely way with the Manager, Information Access & Privacy in relation to investigating and responding to privacy complaints. We also expect complainants to cooperate reasonably and in a timely way with our investigation, including by promptly providing us with information that we might reasonably need to investigate the privacy complaint.

The Office of the Information and Privacy Commissioner has prepared helpful guidance for complaints and a form that may be used to submit privacy complaints to public bodies: see "How to File a Complaint to a Public Body[5]".

Complainants can also request a review of BCA's response to a privacy complaint. The Office of the Information and Privacy Commissioner has provided guidance and a form to facilitate these requests: see "Request for Review/Privacy Complaint Form[6]".

Additional information and assistance can be obtained from the Office of the Information and Privacy Commissioner. Their contact information is:

Office of the Information and Privacy Commissioner
PO Box 9038 Stn Prov Govt
Victoria, BC V8W 9A4

Email: info@oipc.bc.ca
Website: https://www.oipc.bc.ca/

Phone:
250-387-5629 (Victoria)
604-660-2421 (Lower Mainland)
1-800-663-7867 (Elsewhere in BC, ask for transfer to 250-387-5629)

5 https://www.oipc.bc.ca/media/11772/form_complaint-to-public-body.pdf

6 https://www.oipc.bc.ca/media/11778/form_oipc-privacy-complaint-fippa.pdf