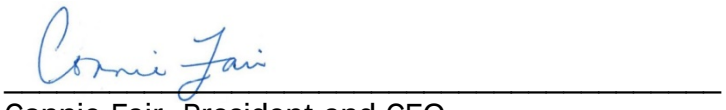
Corporate Policy Statement

TITLE:	**LTSA Personal Information Protection Policy**
ISSUANCE:	LTSA Executive
IMPLEMENTATION:	All LTSA and subsidiary personnel
EXECUTIVE APPROVAL:	 Connie Fair, President and CEO
EFFECTIVE DATE	February 5, 2020
VERSION:	7.0
RELATIONSHIP TO PREVIOUS POLICY:	Amendment to August 8, 2017 (Version 6.0)
FILE NUMBER:	940-00

DOCUMENT REVISION HISTORY

Date	Description of Change	By	Version
2006-10-27	First version of policy established.	G. Archbold	Version 1.0 Signed 2007-01-10
2009-11-25	Housekeeping amendments: • clarify registry vs register language • change position title for designated Privacy Officer • ARCS file classification update	G. Archbold	Version 2.0 2009-11-25
2011-03-16	Revised for compliance with *Freedom of Information and Protection of Privacy Act*	G. Archbold	Version 3.0 2011-03-16
2014-04-29	Revised to reflect: 1. Amendments to FIPPA 2. Operation of myLTSA	G. Archbold	Version 4.0 2014-04-29
2017-04-01	Revised in relation to the LTSA's Privacy Management Program.	C. Fair	Version 5.0
2017-08-08	Revised in relation to the adoption of the IT Cryptography Policy	C. Fair	Version 6.0
2020-02-05	Revised to reflect: 1. Distinct privacy obligations of LTSA and corporate subsidiaries 2. Implementation of Land Owner Transparency Registry	C. Fair	Version 7.0

CONTENTS

1. Purpose and Scope

This policy describes the principles and practices that the Land Title and Survey Authority of British Columbia (LTSA) and its subsidiaries follow to protect personal information.

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

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) and the *Personal Information Protection Act* (PIPA), as applicable.

2. Background

FIPPA and PIPA set out the ground rules for how public bodies may collect, use and disclose personal information. The LTSA was designated a public body for the purposes of on July 13, 2010. Currently no subsidiary corporation of the LTSA is designated as a public body under FIPPA.

In order to carry out its legislated mandate and in operation of its electronic customer portal called "myLTSA", the LTSA collects customer information, some of which may be personal information, as follows:

a. LTSA collects, uses and discloses information from applications and disclosures that are submitted to its statutory decision makers under the *Land Title Act, Land Act* and (in the near future) *Land Owner Transparency Act* (LOTA). The registries established under these statutes are open to the public, who may search and inspect records they contain, including the personal information in those records. For those records that are available for purchase by the public, there is no right to access them under FIPPA (see section 3(1)(j) of FIPPA). Requestors will be re-directed to the access processes for these records that the LTSA has established (front counter and myLTSA services).

b. LTSA collects and uses information provided by myLTSA customers as part of their registration procedures for a myLTSA Customer Account. The registration procedure for a myLTSA Customer Account includes acknowledgement of consent to 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, the LTSA 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.*

  See http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
- *Land Title and Survey Authority Act*.
  See http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_04066_01
- Operating Agreement with the Province.

See http://www.ltsa.ca/docs/Operating-Agreement.pdf

- LTSA Website Statements:
  Terms of Use: https://ltsa.ca/terms-conditions
  Privacy Statement: https://ltsa.ca/privacy

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 have their title or interest in land registered through applications or disclosures under the *Land Title Act*, the *Land Act*, or the *Land Owner Transparency Act* and/or have a myLTSA Customer Account.

myLTSA - The LTSA's electronic customer portal:

- Hosting its Electronic Search and Filing services. Customers must set up myLTSA Enterprise or Explorer accounts in order to electronically transact with the LTSA.
- Providing customer and deposit account management services.
- Facilitating the LTSA's fee collection and remittance services.

Privacy Officer – The employee designated by the CEO to provide advice and take steps aimed at ensuring the LTSA's compliance with its duties and responsibilities as a public body under FIPPA.

Personal Information – Information about an identifiable individual. For example, personal information includes information about a person's name and age; home address and phone number; race, ethnic origin, sexual orientation; medical information; income; marital status and religion; education; employment information. Personal information does *not* include Contact Information.

5. Collecting Personal Information

In carrying out its statutory mandate, the LTSA collects information, some of which may be personal information, from its customers that is necessary to:

- Operate British Columbia's land title and survey systems and process requests for Crown grants that are to be executed by the LTSA;
- Administer the *Land Owner Transparency Act*, including all necessary or advisable activities related to managing, operating and maintaining information systems for the purposes of that Act;
- Deliver requested products and services, including those provided in operating British Columbia's land title and survey systems and processing requests for Crown grants that are to be executed by the LTSA;
- Ensure a high standard of products and services to customers;
- Enable communication with customers;
- Meet statutory and regulatory requirements; and

- Process payments for LTSA's services.

6. Using and Disclosing Personal Information

(a) The LTSA uses and discloses personal information collected from customers for the purposes of carrying out its statutory mandate, including other necessary or advisable activities that relate to its core programs, such as:

- When the LTSA requires legal advice from a lawyer;
- For the purposes of collecting a debt;
- To protect the LTSA and customers from fraud; and
- To investigate an anticipated breach of an agreement or a contravention of law.

(b) The *Land Title Act* provides at s. 377(4) that the land title register is open to the public and may be searched and inspected by any person, subject to reasonable conditions the registrar may impose. The *Land Title Act* authorizes that searches may be made on the basis of individual titles or instruments (by their specific registration number), or by name (s. 377(4)); an owner's contact information may be accessible through such a search.

(c) Long standing approaches to search functionality, and those in place for myLTSA, restrict customer search services (i.e. each search must proceed individually (no ability to search in bulk); the criteria to conduct an individual search is as prescribed in the governing statute (e.g. under *Land Title Act* search is limited to legal description, parcel identifier number, name, title number, charge number or plan number (not civic addresses), on payment of required fees).

(d) When so requested, customers are advised to seek professional advice about how best to avoid collection of particular details on the public land title register.

(e) The LTSA does not sell or provide lists of its customers' personal information to other parties. However, customer information such as name, an address and other property information may be included in public land title registry documents which are open to inspection and search by any person, including the public for a fee pursuant to the *Land Title Act*.

7. Retaining Personal Information

(a) If the LTSA 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 customer has a reasonable opportunity to request access to it.

(b) Subject to policy 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 the LTSA or subsidiary, as applicable, in accordance with its record and retention policies and procedures.

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 their personal information in order to ensure its accuracy and completeness.

A request to correct personal information should be forwarded to the LTSA's Privacy Officer, but if the request relates to personal information appearing in the land title register operated by the LTSA, the request must comply with the *Land Title Act* and be forwarded to the Registrar of Land Titles.

(c) If the personal information which is the subject of a correction request is demonstrated to be inaccurate or incomplete, the LTSA will correct the information as required and send the corrected information to any third party to which the personal information has been disclosed in the previous year. ("Disclosed" as used in this context does not include where a third party has obtained such personal information by conducting a search of the land title register operated by the LTSA.) If the requested correction is not made, the customer's correction request will be noted in the file.

9. Securing Personal Information

(a) The LTSA 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:

- Hard copies of operational land title and survey records are stored in secure vaults with direct physical access to the records limited only to LTSA employees and eligible external parties who have been accredited with direct access privileges under the LTSA's 'Direct Access to Operational Records' policy.
- External parties who are accredited with direct access privileges to the LTSA's operational records are limited to researching registry information that pertains to individual properties/titles. They are not permitted to perform 'bulk searches' or to 'graze' operational records other than that required for a conveyancing, survey, or land title/survey/historical research purpose.
- The LTSA 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 the LTSA Privacy Statement, along with the following LTSA policies:
    - IT Access Control Policy
    - Data Backup Policy
    - Remote Access Policy
    - Information Technology Control: Entity Level Policy
    - Information Security Incident Management Policy
    - IT Security Monitoring Policy

- Mobile Computing Policy
- Wireless Computing Policy
- Information and System Ownership Policy
- Direct Access to Operational Records Policy

- Appropriate security measures are followed when destroying customers' personal information.
- The LTSA requires that third-party service providers that will deal in any way with personal information in the possession of the LTSA enter into contracts whereby the third-party service providers agree to manage all LTSA information in compliance with FIPPA. Use of the LTSA'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 (e.g. USB drives), unless such storage has been approved by the employee's manager based on a clear business need and the device is encrypted in accordance with the IT Cryptography 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 the LTSA, or an employee or associate of a service provider to the LTSA, must take immediate steps to notify the Privacy Officer of any known or suspected privacy breach (as defined in Appendix 1 – Privacy Breach Protocol). The LTSA responds to and manages privacy breaches in accordance with FIPPA and the guidelines set out in Appendix 1 – Privacy Breach Protocol.

10. Public Complaints

The LTSA responds to and manages privacy complaints in accordance with FIPPA and the guidelines set out in Appendix 2 - Privacy Complaint Protocol.

11. Privacy Contact

The LTSA's Privacy Officer is the designated contact person for all inquiries relating to the LTSA's compliance with the requirements of FIPPA.

Inquiries should be forwarded in writing to:

Privacy Officer
Land Title and Survey Authority of BC
Suite 200 - 1321 Blanshard Street
Victoria, BC V8W 9J3
Tel: (250) 410-0600
Email: FOIPPA@ltsa.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 who 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;
- improper disposal of documents containing personal information

The Land Title and Survey Authority (LTSA) is a public body under FIPPA and as such is required to protect the personal information in its custody or under its control as contemplated by 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 the LTSA takes in managing known or suspected privacy breaches and is based on the Office of the Information and Privacy Commissioner's privacy breach management guidelines[2]. The Privacy Officer is responsible for the coordination, investigation and resolution of privacy breaches under this protocol.

Step One: Report and Contain

A privacy breach should immediately be reported to the LTSA's Privacy Officer. The Privacy Officer will assist relevant personnel take immediate steps to contain the privacy breach, including seeking assistance from staff identified by the Privacy Officer (designated staff). Designated staff will cooperate and assist as directed by the Privacy Officer, including to:

- stop unauthorized practice;

[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)

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

The Privacy Officer will keep Executive apprised of any privacy breaches and their management.

The Privacy Officer may also liaise with the Information and Privacy Commissioner with respect to any public comments regarding a privacy breach.

Step One A: Document Breach

The Privacy Officer or designated staff 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;
- ensuring evidence of the privacy breach is preserved;
- prevention strategies and security safeguards.

See Appendix A1 – Privacy Breach Checklist.

Step Two: Risk Evaluation

The Privacy Officer or designated staff will, within two business days of discovering the privacy breach, conduct a risk evaluation to determine whether affected individuals should be notified. The Privacy Officer will consult with the Chief Executive Officer about the outcome of the risk evaluation and the need 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 the LTSA 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:

[3] If the system involves access to statutory services, including the land title register, the Director of Land Titles will provide direction.
[4] See Step 2: Evaluate the risks in the OIPC's *Privacy Breaches: Tools and Resources* for further information on risk evaluations.

- 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 the LTSA, 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 should typically be notified if the privacy breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals. This decision must be made in consultation with the Privacy Officer.

The risk evaluation process, including decisions regarding whether or not to notify, should be documented. See Appendix A1 – Privacy Breach Checklist.

Step Three: Notification

If notification is to occur, it should occur as soon as possible after discovering the privacy breach and ideally no later than one week thereafter unless notification should be delayed in order to not impede a criminal investigation.

The Privacy Officer or designated staff 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 of the Privacy Officer;
- contact information for the Information and Privacy Commissioner.

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

Step Four: Security Safeguards and Prevention Strategies

The Privacy Officer or designated staff will assess whether the LTSA's security safeguards (administrative, physical and technical) are reasonable in light of section 30 of FIPPA.

The Privacy Officer or designated staff 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 A1

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 LTSA (describe for each of the elements below):

j) Loss of public trust and confidence

k) Loss of assets

l) Financial exposure

m) Loss of contracts or business

n) Public safety

o) Breach of contractual obligations

p) Other (specify)

Notification

11. Date and time Privacy Officer 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 of the Privacy Officer

i) Contact information for the Information and Privacy Commissioner

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

a) 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 should typically be notified:

Consider notification if:

b) The personal information involved is sensitive

c) The information has not been fully recovered

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

e) The LTSA requires assistance in responding to the privacy breach

f) The LTSA wants to ensure that the steps taken comply with obligations under privacy legislation:

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. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security)

If the LTSA 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 the LTSA's report.

Appendix 2

PRIVACY COMPLAINT PROTOCOL

A **privacy complaint means** any complaint relating to the LTSA'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 the LTSA.

Privacy complaints should be directed to the LTSA's Privacy Officer by email at FOIPPA@ltsa.ca, or in writing to:

Privacy Officer
Land Title and Survey Authority of British Columbia
Suite 200, 1321 Blanshard Street
Victoria, BC V8W 9J3

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

All personnel must cooperate in a timely way with the Privacy Officer 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 the LTSA'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