Corporate Policy Statement

TITLE:	**LTSA Personal Information Protection Policy**
ISSUANCE:	LTSA Executive
IMPLEMENTATION:	All LTSA and subsidiary personnel
EXECUTIVE APPROVAL	 Al-Karim Kara, President and CEO
EFFECTIVE DATE	September 16, 2022
VERSION:	8.0
RELATIONSHIP TO PREVIOUS POLICY:	Amendment to February 5, 2020 (Version 7.0)
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
2022-09-13	Revised to reflect amendments to FIPPA	D. Leslie	Version 8.0

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 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 *Personal Information Protection Act* (PIPA).

2. Background

Privacy legislation sets out the ground rules for how organizations may collect, use and disclose personal information. The LTSA was designated a public body under FIPPA on July 13, 2010 and takes steps to ensure that all personal information in its custody or control is managed in accordance with the requirements of FIPPA. Currently, no subsidiary corporation of the LTSA is designated as a public body under FIPPA.

In order to carry out its legislated mandate the LTSA collects, uses and discloses information from customers and other members of the public, some of which is personal information. For instance:

a. the LTSA collects, uses and discloses personal information in applications and disclosures that are submitted to its statutory decision makers;

b. the LTSA collects and uses information provided by myLTSA customers as part of the registration procedure for a myLTSA Customer Account.

Wherever personal information is collected, the LTSA provides notice of the reasons for collection and information about how personal information 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

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

4. Definitions

Contact information – Information to 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 considered personal information under FIPPA or PIPA.

Customer – For the purposes of this policy, includes persons who have submitted statutory applications or disclosures to the LTSA, either directly or through a professional, and/or who have a myLTSA Customer Account.

myLTSA - The LTSA's electronic customer portal:

- Hosting its electronic search and filing services. Customers must set up a myLTSA Customer Account 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 be responsible for LTSA's privacy compliance and practices.

Personal Information – Recorded information about an identifiable individual other than Contact Information. For example, personal information includes a person's name and age, home address and phone number, race, ethnic origin and sexual orientation, medical information, income; marital status, religion, education and employment information.

5. Collecting Personal Information

In carrying out its statutory mandate, the LTSA collects information, including personal information, from its customers that is necessary to:

- Operate British Columbia's land title and survey systems;
- Process requests for Crown grants;
- Administer the *Land Owner Transparency Act*;
- Deliver related products and services to customers;
- Create and manage myLTSA customer accounts, including processing payments and ensuring a high standard of customers service.

Whenever the LTSA collects personal information, the individual from whom information is being collected is told the purpose for the collection, the legal authority for the collection and contact information for LTSA's Privacy Officer who can answer questions about the collection.

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 necessary or advisable related services.

(b) The LTSA discloses personal information contained in statutory records as permitted or required under the enabling legislation. For instance, the *Land Title Act* provides that all of the records of the land title register may be searched and inspected by any person and also establishes parameters under which searches may be conducted.

(c) The LTSA's long-standing approach to search functionality related to statutory records, restricts customer search services to ensure that personal information is only disclosed as provided for in the governing statute (e.g. under the *Land Title Act* search options are limited to legal description, parcel identifier number, name, title number, charge number or plan number and only on payment of required fees).

(d) The LTSA does not provide advice to customers about avoiding providing particular details in a statutory application form. When so requested, customers are advised to seek professional advice about their options for submitting applications and registering interests in 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 Section 7(a), an individual's personal information is retained as necessary to fulfill the identified purposes for its collection and in accordance with LTSA's 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.

(b) An individual may request a correction to their personal information in order to ensure its accuracy and completeness. If the request relates to personal information in a statutory record the request must comply with the applicable enactment and should be forwarded to the responsible statutory decision maker. All other requests should be forwarded to LTSA's privacy officer.

(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:

- Physical copies of operational land title and survey records are stored in secure vaults with direct physical access to the records limited to LTSA employees and accredited external parties (see LTSA's 'Direct Access to Operational Records' policy).
- External parties who are accredited with direct access privileges to the LTSA's 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 technologies which are characteristic of mission-critical computer systems. Personal information is protected in accordance with the LTSA Privacy Statement, along with a suite of security-driven policies:
    - Information Security Policy
    - Application Security Policy
    - Data Security Classification Policy
    - Information Security Risk Management Policy
    - IT Cryptography Policy
    - IT Vulnerability Management Policy
    - IT Access Control Policy
    - IT Data Backup Policy
    - IT 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 securely 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 and the Information Security 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 made in writing to:

Privacy Officer
Land Title and Survey Authority of BC
Suite 200 - 1321 Blanshard Street
Victoria, BC V8W 9J3
Email: FOIPPA@ltsa.ca

Appendix 1 – Privacy Breach Protocol

A **privacy breach** occurs when there is unauthorized access to or collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention Part 3 of FIPPA. 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 it;
- unauthorized access to a system or to personal information and/or storage of that personal information;
- unauthorized 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 of British Columbia (LTSA) is a public body under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and as such is required to protect the personal information in its custody or under its control as contemplated by section 30 of FIPPA.

Section 30 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 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 Privacy Breach 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[1]. The Privacy Officer is responsible for the coordination, investigation and resolution of privacy breaches under this protocol.

Step One A: Report and Contain

Where a suspected or known privacy breach has occurred, relevant personnel must take immediate, common-sense steps to limit the breach, including:

- Report the privacy breach immediately to the LTSA's Privacy Officer. The Privacy Officer will assist relevant personnel in taking steps to contain the breach in accordance with requirements in FIPPA.

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

- Contain the breach by (for example):
    - stopping the unauthorized practice;
    - recovering the records;
    - shutting down the system that was breached;
    - revoking or changing computer access codes;
    - correcting 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 Office of the Information and Privacy Commissioner (OIPC) with respect to any public comments about the privacy breach.

Step One B: Document Breach

The privacy breach must be documented and evaluated, 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.

The LTSA documents any potential or known privacy breach using a Privacy Breach Checklist (See Appendix A1 – Privacy Breach Checklist). The Privacy Breach Checklist is completed by personnel with first-hand information about the breach and reviewed by the Privacy Officer.

Step Two: Risk Evaluation

Once the material facts are known the Privacy Officer will 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.

Step Three: Notification

Generally, the IPC and all affected individuals must be notified if the privacy breach could reasonably be expected to result in significant harm to the individual including identify theft or significant:

- bodily harm;
- humiliation;
- damage to reputation or relationships;
- loss of employment, business or professional opportunities;
- access to assets;
- financial loss;
- negative impact on a credit record;

- breach of contractual obligations; or
- hurt, humiliation, embarrassment and damage to reputation or relationships.

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

The Privacy Officer will also consider if other individuals or organizations should be notified:

- Police: if theft or other crime is suspected;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies;
- Other: internal or external parties identified in the investigation and risk analysis (*e.g.* third-party contractors, internal business units, unions).

Notification should occur as soon as possible after discovering the privacy breach unless there is an identified, compelling reason to delay (e.g. where notification would impede a criminal investigation).

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.

Information about how to notify the IPC can be found at: Report a privacy breach (oipc.bc.ca).

Step Four: Security Safeguards and Prevention Strategies

The Privacy Officer in consultation with LTSA's Corporate IT department will assess whether the LTSA's security safeguards (administrative, physical and technical) are reasonable in light of section 30 of FIPPA including whether additional preventative measures should be considered. 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 Day, Year]

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. Individuals affected (or class/type of individuals):

B. Personal Information Involved

7. Describe the personal information involved:

C. Safeguards

8. Describe physical security measures in place (locks, alarm systems, etc.):
9. Describe the technical security measures in place (encryption, password protection, other):
10. Describe the organizational security measures in place (security clearances, policies, role-based access, training programs, contractual provisions):

D. Harm From the Breach

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

To individuals (describe for each of the elements below or mark N/A)

a) Personal safety:
b) Identity theft or fraud:
c) Access to assets:
d) Financial loss/exposure:
e) Loss of business or employment opportunities:
f) Breach of contractual obligations:
g) Hurt, humiliation, embarrassment:
h) Other (specify):

To LTSA (describe for each of the elements below or mark N/A):

a) Loss of public trust and confidence:

b) Access to assets:

c) Financial loss or exposure:

d) Loss of public trust and confidence:

e) Loss of contracts or business:

f) Breach of contractual obligations:

g) Other (specify):

E. Notification

12. Date and time Privacy Officer was notified:

13. Have affected individuals been notified?

    a) If "yes" who (or what class) has been notified and when?

    b) If "no", will they be notified and when?

14. Have the police or other third parties been notified (e.g. professional bodies or persons required under contract)?

    a) If "yes", who was notified and when?

15. 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) Other (e.g. risks to the individual, steps taken to the control the harm, future steps planned to prevent further privacy breaches, steps the individual can take to control or reduce the harm, contact information of Privacy Officer &/or Information and Privacy Commissioner).

16. Should or must the Office of the Information and Privacy Commissioner be notified of the Breach? [refer to Privacy Breach Protocol]

    Notification may be required 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) LTSA requires assistance in responding to the privacy breach;

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

F. Prevention

17. 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)

18. 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