Privacy Management Audit Plan

The Privacy Officer for the Land Title and Survey Authority (LTSA) will monitor, audit, and revise the effectiveness of program controls where necessary. This process will include:

Every 24 months, or more often if circumstances require, the Privacy Officer will review:

- the privacy related policies, procedures and practices;
- the personal information inventory to ensure that new collections, uses and disclosures of personal information are identified;
- personal information banks;
- privacy training materials;
- privacy impact assessments and related policies and practices;
- agreements involving the collection, use and disclosure of personal information;
- information sharing, research, data-linking and common and integrated program agreements; and
- privacy related external communications.

See: Appendix 1 - Audit Checklist.

Revisions to privacy related policies, procedures and practices, the personal information inventory, personal information banks, privacy training materials, privacy impact assessments, agreements and external communications will be made as needed following a compliance review, in response to a privacy breach or privacy complaint, new guidance, industry-based best practices or as a result of environmental scans.

Information systems staff, in consultation as necessary with the Privacy Officer will review the controls the LTSA has in place for systems, including those that contain personal information. Information systems staff will review the Information Systems Audit Checklist in Appendix 2 every 24 months.

The Privacy Officer will ensure that necessary information is recorded and retained in relation to any compliance review to support any recommended actions and future compliance reviews.

Appendix 1 - Audit Checklist

Review of:

- ☐ FIPPA and other relevant statues and regulatory requirements to ensure Privacy Management Program, and LTSA policies, practices and procedure continue to align with these statutes and requirements and recommend any necessary revisions.
- ☐ Privacy Policies and recommend any necessary updates
- ☐ Personal information inventory and personal information banks to ensure that new collections, uses and disclosures of personal information are identified and documented
- ☐ Logs of employee privacy training to ensure all employees have current training
- ☐ Privacy training materials and update as necessary
- ☐ Privacy impact assessments to determine if any updates are required
- ☐ Agreements involving the collection, use and disclosure of personal information and make recommendations for necessary revisions
- ☐ Information sharing, research, data-linking and common and integrated program agreements to determine if any updates are required; and
- ☐ Privacy related external communications.

Appendix 2 - Information Systems Audit Checklist

IT Security Audit Program

- ☐ Any system/audit logs that relate to the handling of personal information are, if applicable, securely stored and accessed.
- ☐ Monitor any existing system/audit logs for alerts on suspicious activities or other types of security event.

Ongoing Audits

- ☐ 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.
- ☐ Backup procedures of the database management systems to ensure data recoverability and integrity.
- ☐ Access controls ensure that personal information that is passed between computers, or between discrete systems is appropriate.

Scheduled Audits

- ☐ Software/hardware inventory maintained and up-to-date.
- ☐ No storage media contain personal information, all personal information is stored on secure servers.

Audit Verification

- ☐ Audit monitoring and review of access settings, to detect errors in access rights (including through confirmation with the business owner of accounts).
- ☐ Ongoing security evaluations and vulnerability assessments.

Audit Implementation

- ☐ Review of audit results and recommendations and implement necessary revisions in alignment with business needs.