BC ASSESSMENT

Privacy Management & Accountability Audit Plan

The Manager, Information Access & Privacy may conduct compliance reviews in order to assess compliance with FIPPA and this and other BCA policies, practices and procedures relating to BCA's PMAP. Every 24 months, or more often if circumstances require, the Manager, Information Access & Privacy will review:

- the PMAP and other 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 the PMAP, other 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.

The Senior Security Analyst, ITS will coordinate security threat and risk assessments to ensure security risks in relation to personal information are identified and addressed on an ongoing basis. This includes those prepared in relation to PIAs.

The ITS Senior Security Analyst and the ITS Service Operations Manager, in consultation as necessary with the Manager, Information Access & Privacy, will review the controls BCA has in place for systems, including those that contain personal information. The ITS Senior Security Analyst, ITS Service Operations Manager and Manager, Information Access & Privacy will review the Information Systems Audit Checklist in Appendix 2 every 24 months.

All BCA employees must assist the Manager, Information Access & Privacy with these reviews.

The Manager, Information Access & Privacy will ensure that necessary information is recorded and retained in relation to any compliance review to support any recommended actions and future compliance reviews.

2. Privacy Contact

Advice on this PMAP may be obtained from

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

Phone: 1.866.825.8322

Email: access&privacy@bcassessment.ca

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

APPENDIX 1: AUDIT CHECKLIST

Review of:

- ☐ FIPPA and other relevant statutes and regulatory requirements to ensure Privacy Management and Accountability Program, and BCA policies, practices and procedure continue to align with these statutes and requirements and recommend any necessary revisions.
- ☐ Privacy Management and Accountability Policy, Personal Information Protection Policy and Employee Personal Information Protection Policy 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.
- ☐ 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) 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 portable storage media contain personal information, all personal information is stored on secure servers [unless 9(b) limited exception applies].

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.