EAB Tribunal Cluster
Fourth Floor, 747 Fort Street, Victoria BC V8W 3E9
Tel: (250) 387-3464 **Fax: (250) 356-9923**
www.bceab.ca **Email: info@bceab.ca**

Privacy Management Program

Introduction

This privacy management program sets out privacy-related processes and procedures for the Environmental Appeal Board, Forest Appeals Commission, and Oil and Gas Appeal Tribunal (any and each of which is referred to as the "Body"). Each Body is overseen by a Chair (the "Chair").

Individual Responsibilities

Within the Body, the Chair is responsible for supporting the development, implementation, and maintenance of privacy policies and procedures, and for supporting the Body's compliance with the *Freedom of Information and Protection of Privacy Act*.

The Vice Chair, Service Delivery is the appropriate point of contact in first instance, for privacy-related matters such as privacy questions or concerns.

Privacy Impact Assessments

When undertaking any project or program that involves the collection, storage, use, or disposal of personal information, the Body will perform a Privacy Impact Assessment (PIA). A PIA includes 26 questions that encourage one how to reduce risk and protect privacy in a project. PIAs are available in standard form online.

When a PIA is complete, the Body will save a copy in accordance with its document retention schedule.

Information Sharing Agreements

The Body will engage in information-sharing agreements in any instances where it regularly, systemically shares personal information with a person or organization, other than a public body as defined in the *Freedom of Information and Protection of Privacy Act*.

Privacy Complaints

Anyone with a privacy-related complaint or concern should forward them to the Body's general email or mailing address, both available on its website. The email will be forwarded to the appropriate personnel to respond, who will follow up for further information, or to discuss the complaint or concern, as soon as possible.

Should the concern or complaint reveal a privacy breach, the process described below takes place. Should the concern or complaint reveal a systemic weakness in the Body's collection, storage, use, or disposal of personal information, the Body will consider how to improve its processes. If the Chair considers it appropriate, they may also require that a PIA be undertaken with respect to the process at issue (as described above).

Privacy Breaches

A privacy breach is any:

- theft or loss of, or
- any access, collection, use or disclosure of

personal information in the Body's custody or control, not authorized under the *Freedom of Information and Protection of Privacy Act*. Where a Body becomes aware of a privacy breach, the Chair will be notified as soon as possible. The Chair will assess whether the breach is likely to result in significant harm to the person whose information has been disclosed. The assessment involves considering:

- the nature of the person who was the subject of the breach,
- the nature of the information disclosed,
- whether there is an expectation of privacy related to the information,
- to whom the information was disclosed,
- the relationship between the person who was the subject of the breach and the person(s) to whom the information was disclosed,
- any steps the Body can take to mitigate the risk to the person who was the subject of the breach, and
- any other factors the Chair considers relevant.

If the Chair determines that significant harm is likely to result from the breach, they will notify the person who was the subject of the breach and the Freedom of Information and Protection of Privacy Commissioner. Notifications of the person who was the subject of the breach are typically done in writing, but may be done via telephone, with a follow up in writing, if:

- the risk of harm is particularly urgent,
- there is likely to be significant delay in the person receiving or understanding the notification in writing, or
- for any other reasons the Chair considers significant.

Privacy Education and Awareness

Training in the appropriate collection, storage, use, and disposal of personal information forms part of the onboarding and training of all new staff and members, within the context of their roles. This training will be reinforced as needed, including where any new systems or procedures involve the collection, storage, use, or disposal of personal information, but at least once per year.

Privacy Policies and Procedures

All privacy policies and written practices or processes are made electronically available to all employees and members. Storage locations will be communicated as part of the onboarding and regular training on privacy-related procedures. These policies and procedures are also available to the public, on the Body's website.

Service Providers and Privacy

Where any service providers deal with the collection, storage, use, or disposal of personal information, they must comply with any information sharing agreements that form part of the project or service being undertaken, and any safeguards arising from the PIA (as discussed above).

At the start of any work, the relevant contact for the service provider, within the Body, will confirm the service provider's understanding and acceptance of these requirements.

Monitoring and Updating

The Chair will review this privacy management program annually, to ensure it is relevant and effective, in identifying and avoiding risks to the protection of privacy, and in identifying, mitigating, and addressing any privacy breaches that take place. The Chair will update this program as needed to ensure compliance with the needs of the *Freedom of Information and Protection of Privacy Act*.