ALBERTA EMPLOYMENT, IMMIGRATION AND INDUSTRY

PRIVACY POLICY

Alberta Employment, Immigration and Industry

May 2007

Philosophy Statement:

> ***"Alberta Employment, Immigration and Industry is committed to managing information in an open and transparent manner, while respecting the privacy of Albertans."***

Principles:

- *AEII is a caretaker of the personal information it manages.*
- *Individuals should be the first choice as a source for the provision of their information.*
- *Individuals own their own personal information, and as such, have an established right of access to it.*
- *Individuals have a right to be properly notified regarding the use and potential flow of their personal information.*
- *AEII will collect only the minimum amount of personal information necessary to undertake its responsibilities.*
- *Individuals have a right to know how and where their personal information may be disclosed.*

PRIVACY POLICY

Whenever information is being handled, regardless of its form, there are certain expectations that must be met. These expectations are not in place of, but rather are enhancements to, the privacy legislation.

The first set of expectations focuses on the manner in which Departmental staff is expected to manage the privacy of personal information.

The second set focuses on the manner in which general (non-personal) information is dealt with within the Department.

Who does the policy apply to?

The policy applies to all staff within the Department, all agencies and their staff and any others working or providing services on behalf of the Department. References to staff within this policy and related documents will include all of the above.

Staff are expected to adhere to the policy as they perform the functions that they are responsible for. Any exceptions to the Policy require formal approval. (**See** Appendix A).

A. Personal Information

1.0	Personal information will be treated with the respect that is due, given the principle of custodianship.

1.01 The privacy of an individual is maintained by respecting the privacy of their personal information that is under the control and custody of the Department.

- All staff have an obligation to ensure that they maintain confidentiality as they collect and use the personal information of the individuals that they work with and provide services to.
- Attention should be given to not engaging in discussions of third party personal information in areas where there is potential for the conversations to be overheard.
- Similarly, attention should be given to limiting the access that may be inadvertently provided to documents, files and electronic records.

1.02 Collection of personal information should be undertaken in a confidential manner, which includes attending to the physical environment.

- Steps should be taken to minimize the risk of disclosing personal information through interviews that are conducted in an open environment. The set-up of facilities for Departmental staff should therefore take this into consideration.

What are the rights of clients vis-à-vis their information?

2.0	Individuals whose personal information is collected and maintained by the Department have a right of access to that information.

2.01 Individuals should be clearly advised regarding their right of access.

- Individuals whose information is in the custody of, or under the control of the Department, generally have a right to access that information, subject to specific and limited exceptions under the *Freedom of Information and Protection of Privacy* (FOIP) *Act*.
- Staff should be generally familiar with an individual's right of access as it pertains to the personal information that the staff is responsible for.

2.02 Individuals should also be provided direction on the manner by which they may be able to access their information.

- Direction should be readily provided to individuals regarding the means by which they may be able to access their personal information, whether through an informal or a formal (FOIP request) process.
- Certain documents may have a cost attached to producing copies. It may be reasonable to pass some of the cost on to the consumer. (*Note: A decision needs to be made on how the costing would be determined, and by whom.)* ***See also B 1.03.***

3.0	Individuals whose personal information is being collected have a right to know how and where that information will be used.

When do we require notification?

3.01 Departmental staff (and agents) involved in the collection of personal information are required to provide proper notification to individuals as to why their information is

required, how it will be used, and with whom it may be shared. (**See also** #4, Proper Authority)

- This notification should be provided at the time that the information is collected.
- Being open with individuals about the reasons for collection and the purposes for which their information will be used is consistent with the Department's commitment to transparency and accountability.

3.02 Any forms used in the collection of personal information must have a statement indicating the proper authority for the collection of that information.

- All collection forms being developed should be submitted to Forms and IPO personnel for their feedback.

What do clients need to know? (information flow)

3.03 Personal information that is in the custody of, or under the control of the Department, should be used only for the purpose for which it was collected, or for a use that is consistent with that purpose, or in a manner that is allowed for, or required by law.

- Staff should be able to readily identify the purpose for which they require the personal information that they have responsibilities for collecting and/or using.

3.04 Individuals should also be advised of any indirect collection of their personal information.

- If, as the result of an application for service or benefits there is a requirement to collect or otherwise obtain information about the individual from another source, staff should identify to the client how that information may be collected.
- If this process is identified on collection forms, the language on the forms should be clear and easily understood by the individuals whose information is being collected.
- Exceptions to this may include investigative processes.

What obligation do we have to inform clients on changes to programs? on process?

3.05 Individuals should be advised of changes in how their information may be used.

- The right of an individual to know how their personal information will be used means that changes to the use should be identified as they occur. Decisions on how that is undertaken should include consideration of factors such as the significance of the change, and the ease of reaching the individual. Various means available could include notices attached to monthly benefit statements, or posted on websites.

3.06 Individuals in receipt of benefits or services who may be impacted by changes in the program should be advised of those changes.

- Posting notices may not be deemed to be sufficient, although that decision may be dependent on the degree of change or impact.

3.07 A staff member is obligated to identify the name and position of an official who can answer any questions regarding information management practices as they relate to the individual.

- This may include the name of the staff member responsible for the case management or some other staff who is sufficiently knowledgeable about the information management practices.

What information can be collected?

4.0	Personal information of individuals will only be collected and used if there is proper authority to do so.

4.01 Any programs and services should be able to readily identify the authority that they operate under, and by which personal information can be collected.

- The authority that allows for the collection of information generally flows from legislation. Programs that are not legislated are generally deemed to be operating programs or activities of the Department.
- Authority to collect information may be explicitly stated in the legislation, but is more often implicit.
- Investigative processes that are deemed to fall under the umbrella of law enforcement fall under the third criteria (operating program or activity of a government organization) identified in the *FOIP Act*.
- Contracted agencies or other organizations operating under an agreement, or through some other means conducting business on behalf of the Department, receive their authority by way of the contract or agreement.

4.02 Only the minimum amount of personal information required for the provision of services will be collected. Information that is collected and not required should be disposed of or returned to the individual to whom it pertains, if in the form of a record.

- Personal information should not be collected "just in case" it is needed. Rather, there should be a clearly defined need for the information, without which it would be difficult to deliver the program or service.

How is records management linked to this policy?

5.0	Documentation, whether in paper, electronic or other form, must be managed properly.

5.01 Retention and disposition schedules should exist for all documents, and in all formats.

- This applies not only to paper documents, but also to electronic records, including databases and e-mail messages and attachments.
- Assistance in the identification of retention schedules that may be available, or on the creation or updating of existing schedules, may be obtained from the Records Services staff, Service Alberta.

5.02 Such schedules must be adhered to, including the appropriate purging of electronic records. Any exceptions should be properly requested and documented.

- An information management matrix should readily identify the position responsible for such decisions.

5.03 Files must be stored and managed properly, in a manner that allows for retrieval if required.

- Documents that are related to files but stored separately should be cross-referenced or in some other manner readily identified.

5.04 Updates to software used in the storage of records in an electronic format should allow for the retrieval of data already collected and stored.

- If such retrieval is not deemed to be feasible or practical, consideration should be given as to whether there is a need to retain the information.

How do we ensure that our agents follow the policy?

5.05 Contracts should clearly outline the requirements and expectations placed on agencies regarding the records that they create. Such expectations would include the identification of records that must be submitted to the Department, and those that may be maintained for use by the agency, and for access by Departmental staff.

- Expectations can be identified by means of a separate appendix, or identified within the contract itself.
- Contract managers should understand and monitor the agencies for compliance with the requirements.

Who can we share the information with?

6.0	The appropriately delegated individuals will undertake decisions regarding the collection, use, and disclosure of personal information.

6.01 Staff should have an understanding of how the delegations under the *Freedom of Information and Protection of Privacy Act* apply to them.

- The FOIP delegation matrix provides staff the authority to use and disclose third party personal information in the performance of the duties expected of their positions. Staff should be able to identify their authority as it relates to the use and disclosure of personal information.

Who makes decisions to release/use information? (delegations)

6.02 Should staff not be delegated authority to disclose personal information, they must refer decisions on disclosure to the appropriate level.

- Information regarding the appropriate delegation levels should be readily available to all staff.

6.03 Where agreements regarding the disclosure or sharing of information are entered into, there must be approval at the appropriate level. This also includes approval of research proposals.

- Decisions made regarding entering into agreements should be made at a senior official (division head?) level. Individuals identified as being responsible for the duties identified within the agreement can be at a less senior level.

6.04 A *Research Approval Process* that would ensure responsibility for the review and recommendation of research proposals should be set up.

- The Research Approval Process would ensure that a consistent manner is in place for decision-making that takes into consideration the values of the Department.

What are the rights of staff and stakeholders to access information?

7.0	Staff members are limited to accessing only the information that they require to provide services to individuals, or as otherwise required to carry out the responsibilities of their positions.

7.01 Staff should be restricted to accessing personal information that they require. This restriction applies to information stored in both electronic information systems and paper files.

- Wherever possible, access to various screens should be limited to those that contain the information that the staff requires, based on their positions.

- Where this is not feasible, policies and practices should reinforce the limits placed on access.

7.02 Audit trails should be built in as new systems are developed.
- The ability to audit the access by users to different systems will serve to offer an added level of protection of privacy for individuals.
- This becomes especially important where systems are accessed by individuals outside of the Department, who may operate under a less limiting sphere of control.

7.03 Stakeholders are equally limited to accessing only the information that they have authority to obtain. They may receive this authority in a number of ways, including:
- contracts or agreements; and,
- data or information sharing agreements.

8.0	The collection and documentation of personal information must be undertaken in a complete and accurate manner.

8.01 This must be balanced with collecting only the information that is required and authorized.
- Decisions that affect individuals and the services or benefits that they receive are made on the basis of the personal information that is collected about them. It is therefore incumbent on staff that they collect and record the information in as accurate a manner as is reasonable to expect.
- At the same time, only personal information that is required and authorized should be collected.

When is consent required?

9.0	Informed consent should be used whenever possible, as deemed appropriate.

9.01 Consent is the first option to follow in seeking to share or obtain personal information.
- The determination of eligibility for services and benefits does not necessarily require consent. However, the use of consent should be considered as program areas make decisions on how information will be collected and used. (**See also** 3.0 - notification)
- Sharing or disclosing personal information is often undertaken with a view to delivering services on behalf of the individual in the context of integrated or collaborative partnerships.
- In order to ensure that the individual receiving these services is a part of the process, involving them through a consent-based process is important.

What constitutes consent?

9.02 Informed consent should clearly identify *what* information will be shared or obtained, with *whom*, and for *what* purpose. It should also be *time limited*, wherever possible.
- In order to allow for an individual to provide a proper consent, the individual should be informed with the specific uses of their information and where it will flow.

9.03 Consent should not be used in situations where information will be accessed or disclosed whether or not consent is obtained.
- To undertake such activity negates the validity of a consent-based process, and serves to minimize any trust in the Department.

9.04 Individuals whose personal information is collected should be advised of how the information will be maintained (e.g., retention, security).

- Providing information on retention periods to individuals assists them to understand the degree of control over the information, and allows them to make informed decisions regarding their access to it.

When are we required to document disclosure or sharing?

10.0	Any disclosure of personal information should be clearly documented.

10.01 A document trail should exist in order to identify where information has been disclosed or shared. This serves a number of purposes:

- If information is shared, individuals have a right to know with whom it has been shared.
  - This continues to provide an assurance of transparency and accountability.
- If information needs to be corrected, there is an obligation to ensure that the corrections can follow the disclosure.
  - This reflects compliance with a provision contained in the FOIP.
- Requests for information can readily identify other locations for information storage.
  - The Department has an obligation to respond to requests for information in as complete and accurate a manner as possible. It is therefore necessary to be able to identify all records that relate to such requests.

How do we secure information?

11.0	All personal information must be maintained in a secure manner.

Who can access records?

11.01 Access to personal information has to be according to requirements as per **A 6.0**.

- Access to specific file information should be limited to staff who require it in order to perform their responsibilities.
- Access should be restricted in keeping with security requirements.

11.02 Electronic systems should be safeguarded from breaches in all areas.

- The proper use of identifiers (ids) and passwords must be followed in order to properly control and limit access. This requires that ids not be shared.
- The use of back-ups must be followed.
- The use of computers in the home, laptops, and dial-up id's should only be undertaken with adherence to accepted Departmental procedures.

11.03 The Departmental Security Policy must be adhered to.

- Staff members have a responsibility to familiarize themselves with the policy and understand how it applies to their circumstances.

11.04 The transfer of any personal information (e-mail, fax, Internet) by electronic means should be restricted to secure methods wherever possible.

- Caution must be used when transmitting any sensitive information via electronic means.
- There may be occasions when the risks of not sending sensitive information may outweigh the risks of doing so. However, there will be very limited circumstances when the risk of breaching privacy is offset by the efficiencies gained in sending information through a non-secure means.

11.05 Paper files are also to be managed with the appropriate care.

- Attention must be given to following the proper procedures regarding paper file storage, transportation, and disposition.

What are the consequences for policy breaches? (internal and external)

12.0	Any loss of personal information or breach of personal privacy is considered to be a sensitive breach, and shall be immediately reported.

12.01 Individuals have a right to know that their information has been lost or improperly obtained.

- When documents containing personal information have been lost, the Department has lost any ability to control how that information may be used. In such cases, the Department has a responsibility to at least consider the appropriateness of advising the individual to whom the information pertains.
- Decisions on whether or not to advise the individual should be documented along with the rationale.

12.02 Inadvertent disclosures are best dealt with in an open manner.

- Such incidents should be reported to the designated senior official and to the Director, Information and Privacy Office. Reports should outline:
  - the circumstances that led to the inadvertent disclosure or loss;
  - the steps taken to recover the documents; and,
  - recommendations to prevent the likelihood of the circumstances being repeated, if appropriate.
- Disciplinary action may be warranted in situations where there has been misconduct, illegal use or illegal collection - such instances would be referred to the appropriate division/branch head.
  - Staff members need to understand that the Department is committed to the custodianship it has over personal information, and of the role they have in the need to protect it properly.
- Penalties will generally not be levied where policy has been followed or where there have been reasonable steps taken to protect the information.
  - There has to be recognition that there may be occasions where circumstances beyond the control of staff have played a part in disclosures.

B. General Information

This section is in addition the section on Personal Privacy. It focuses on the manner in which information that is not the personal information of a third party is dealt with, in addition to **Part A.**

When do we release information either formally or informally?

1. The Department is committed to being open and transparent.

1.01 The rule of thumb to follow is to allow for the disclosure of general information unless there is a solid reason not to.
- While there are a number of provisions within FOIP that allow for information not to be disclosed, they should by and large be the exception rather than the rule.

1.02 Information may be classified as being available to the public, or as requiring access through a formal FOIP request.
- The classification of information in this manner will assist the public in identifying the route by which they should request information.
- It will also serve to assist staff in responding to inquiries for information.

1.03 Even where it is available to the public, there should be some decision as to how that will be undertaken:
  - active dissemination;
  - available through the library;
  - available at a cost; and,
  - only available on request (on an informal basis).
- Certain documents may be 'pushed' out into the public domain. Many of these may be available as news releases or postings through the Internet and placed in the Department's library.
- Certain documents may have a cost attached to producing copies. It may be reasonable to pass some of the cost on to the consumer. {*A decision needs to be made on how the costing would be determined, and by whom.}* ***See also A 2.02.***

2. All policies and procedures should generally be available to the public.

2.01 Policy manuals should be available either through the Internet or through a series of access points across the Department.
- This applies to all policy manuals and associated directives that are used to assist in the decision-making process when the decisions may impact on an individual being provided services and/or benefits.
- It does not necessarily apply to procedure manuals that outline the process rather than the decisions made. However, if there are no concerns in making these available to the public, they should be included as well.

2.02 The rationale for decisions made should be clearly laid out and supported through well-developed processes. This is especially true of appeal processes.
- The demonstration of such a process serves to develop a sense of consistency and trust in the process.

3. Staff should readily identify themselves to the individuals that they are working or dealing with.

3.01 Staff members are required to identify the name and position of an official who can answer any questions regarding information management practices as they relate to the situation.

- The individual staff identified here may often be the case manager involved with the delivery of services and/or benefits to the individual.
- In other situations, it may be appropriate to identify a specialist or some other expert resource person.

What controls do our clients have over the information flows and processes?

4. Individuals should be clearly advised of what services and options are available to them.

4.01 Information on appeal mechanisms should be readily available to individuals and organizations.

- The information that relates to the ability to appeal a decision should be posted or otherwise made available (**See also B 2.01**).
- In addition to the above, individuals should be provided with the information that they require on the subject matter they are appealing. This could include the relevant program policy or legislation, as well as the rationale that the Department has used in arriving at its decision.

4.02 The process of accessing information by an individual or organization should be clearly set out and available. This includes formal (FOIP requests) and informal processes.

- Forms used by the Department to request information should be readily available via a number of access points.
- Information on the individuals' rights of access and the methods available to them could also be provided concurrent with any intake process.

4.03 Individuals have a right to request information and, if appropriate, obtain it in as simple a process as possible.

- In order to promote transparency and accountability, it is important to remove any semblance of barriers to access.

5. The manner in which information will be handled and dealt with should be clearly identified to all individuals and organizations that have involvement with the Department.

5.01 No guarantees should be given that information submitted "in confidence" will be maintained as such. Requests to maintain confidence may be honoured to some degree, subject to the applicable legislative requirements.

- The Department needs to be able to allude to a certain degree of confidentiality as it makes decisions on a variety of areas, including policy development and draft legislation.
- Documents that are submitted regarding such processes may be afforded a degree of confidence, but decisions should be made that clearly outline the circumstances under which this would be undertaken.
- Should such confidentiality be exercised, the Department should consider at what point it might no longer be required, and identify that in its process as well. For example, if submissions to the Department are to be considered as confidential due to their considerations in the development of new legislation, once the decisions are made and the legislation introduced/passed, the information considered in the

development may be subject to public scrutiny. This process would allow for deliberations to be undertaken in a closed approach, but the objectives of transparency would be met by the publication of the considerations in due course.

5.02 Individuals who raise a complaint should be advised that in order for the Department to investigate, the individual/organization being investigated might be able to identify the complainant through the context and the review.

- Given this, individuals should not be advised of any guarantees of confidentiality.
- Assurances may be provided, however, that the Department will try to maintain whatever confidentiality is possible. The specific identity of the complainant is not generally provided.
- Requests made under FOIP are generally processed in such a way that the identity of a "reporter" or complainant is excepted from disclosure. The Department is interested in ensuring that individuals can continue to raise concerns or issues in a variety of areas. If individuals do not feel that they can raise concerns in a relatively confidential manner, they may not feel that it is safe to complain.

5.03 Information that is submitted to Departmental programs and delivery areas may be subject to FOIP requests. Factors to be considered that would assist in the decisions on the disclosure of such information should be outlined in advance, wherever possible.

- When the Information and Privacy Office receives a request for information, it has an obligation under the *FOIP Act* to assist the applicant in obtaining the information that they are requesting. The provision of the records is subject to limited exceptions to disclosure. The application of those exceptions can be facilitated through the identification of areas that may be considered under such an exception. Examples may include:
  - identifying legal opinions or other documents that may be subject to client-solicitor privilege;
  - information that should be deemed as advice, deliberations or analysis; and,
  - information that is considered the business information of a third party.

Additional interpretation on the impact of the Privacy Policy is available through the Information and Privacy Office.

See the Attached Glossary of Terms for definitions of terms used.

Alberta Employment, Immigration and Industry
Privacy Policy Exception Process

Introduction:

Alberta Employment, Immigration and Industry is responsible for the management of the information, both personal and general that it has under its control and custody. The AEII Privacy and Security Policies *(under development)* provide a set of standards on how the Department will ensure that the information is dealt with in an appropriate manner. As with any policies, there may be limited and specific occasions where there is a need for the departure from the accepted standards. In order to maintain its accountability, a decision has been made that a formal process of approving these exceptions be undertaken.

Process:

- A request for exception should be presented outlining the area of policy in which an exception is being requested. It should include the rationale, the potential impacts both for and against, and the length of time for which the exception is being requested.
- Decisions will be made by the division head responsible for the unit/branch requesting the exception.
- The Division Head could rely on resources from within their own division, and including other relevant areas, including Information Management and Technology, Information and Privacy, and Legislative Planning.
- Any exceptions need to be documented and stored in a central location.

GLOSSARY OF TERMS

Accountability	• The recognition that specifically, the Department and the staff are responsible to the individuals and organizations it provides services to, and generally, to the public at large.
Agents	• Individuals or organizations working on behalf of, or representing another individual or organization.
Case Management	• The responsibility of a staff for the services and benefits being delivered to individuals and organizations on behalf of the Department. It includes the proper recording and documentation of the information relating to the delivery.
Consent	• The process of agreeing to an activity or process. In the context of privacy, it refers to an agreement in writing to the collection and/or use of information. (**See also** *Informed and Prescribed Consent*)
Control and Custody	• Refers to the records that the Department has the ability to regulate through its authority (e.g., via contract, agreement, or legislation) if in the physical possession of an external entity, or to records that it has in its custody.
Custodian	• Individual or organization responsible for the information that is maintained or controlled by the Department, regardless of format.
Dial-up id's	• Refers to the electronic identification process that allows an external computer (laptop, home PC) the ability to log on to the Departmental systems.
Exceptions	• Refers to the provisions within the FOIP legislation that allows the Department to not disclose specific records. These are limited and specific and may be either mandatory or discretionary.
FOIP	• *Freedom of Information and Protection of Privacy Act.*
FOIP Delegation Matrix	• A table that outlines the delegation of responsibility for the various provisions of the Act. It forms a part of the Delegation and Transfer of Responsibility signed by the Minister.
FOIP Request	• A formal request for information made under the FOIP Act. Such a request must be submitted in writing, indicating that it is a request being made under the Act.
Information Management	• The process of ensuring that the information maintained on the electronic and paper files is handled in an appropriate fashion. • Note: This entails a number of areas of responsibility, including all divisions of the Department.

Informed Consent	• A consent that is provided by an individual only once they have been made fully aware of the information that relates to the activity to which they are being asked to agree to. (**See also** *Consent and Prescribed Consent*)
Notification	• The process of ensuring that individuals and organizations are made aware of information and processes that may impact on them. Generally, refers to ensuring that they are aware of the guidelines or practices that relate to the information that is collected from and about them.
Personal Information	• Any information that relates to an individual, including personal identifiers and information that through context may also identify an individual (**See also** definition of personal information in FOIP).
Prescribed Consent	• Consent that has been provided in accordance with the FOIP Regulations. It must identify what personal information will be shared, with whom, and for what specific purpose. It is also suggested that it include a time element.
Purging	• The removal of information from an electronic system.
Records Management	• The processes that are in place to ensure the proper method of dealing with records. It applies to both electronic and paper (hard copy) records.
Right of Access	• Individuals and organizations may establish a right to obtain or view to information that is held in the records that come under the control and custody of the Department.
Service Alberta	• Service Alberta - responsible for the delivery of a number of administrative services across government Departments, including human resources, payroll, budgeting and financial management support, records services, and libraries.
Staff	• Includes individuals working for the Department, and, for the purpose of this policy, any individual or organization working or providing services on behalf of the Department, through contracts, agreements, or other arrangements.
Transparency	• Ensuring that the activities that the Department undertakes in relation to the use of information are open to public scrutiny.