



(& Affiliates)

PRIVACY CODE

Table Of Contents:

1. Principle 1 - Accountability
2. Principle 2 - Identifying Purposes
3. Principle 3 – Consent
4. Principle 4 - Limiting Collection
5. Principle 5 - Limiting Use, Disclosure, and Retention
6. Principle 6 – Accuracy
7. Principle 7 – Safeguards
8. Principle 8 – Openness
9. Principle 9 - Individual Access
10. Principle 10 - Challenging Compliance

For additional information, contact:

**Chief Privacy Information Officer
Bruce Haines
Independent Investigative Services Inc. (IIS)
(formerly Haines, Miller & Associates Inc.)
290 North Queen Street, Suite 215
Toronto, Ontario M9C 5L2
Tel: (416) 241-0009 x 224
Fax: (416) 241-9737
Email: bhaines@hainesmiller.com**

Independent Investigative Services Inc. (IIS & Affiliates)

Privacy Code

Through its network of private investigators and consultants, IIS values its relationship with its customers and employees, and is committed to the protection of their personal information. Accordingly, IIS adheres to the privacy principles, and accompanying commentary, set out below (the "Privacy Principles"). The Privacy Principles are based on the principles set out in Schedule 1 of the Personal Information Protection and Electronic Documents Act (Canada) (the "Act"). "Personal Information", as used in this Code, means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Principle 1 - Accountability

IIS is responsible for all Personal Information under its control.

Accountability for our compliance with the Privacy Principles rests with our Chief Information Officer, even though all individuals within IIS have responsibility for the day-to-day collection and processing of Personal Information and may be delegated to act on behalf of the Chief Information Officer.

Our organization has taken appropriate measures to develop procedures to: (a) protect personal information; (b) receive and respond to complaints and inquiries; (c) train our employees about policies and practices relating to the protection of personal information; and (d) distribute information explaining our policies and practices relating to the protection of personal information.

We are responsible for Personal Information in our possession or custody, including information that may be transferred to a third party. We will use contractual or other means to provide a comparable level of protection when a third party is processing the information.

Principle 2 - Identifying Purposes

We will identify and document the purposes for which we collect, use, or disclose Personal Information at or before the time of collection.

The purposes will be limited to those which are related to our business (investigative and consulting services) and which a reasonable person would consider appropriate in the circumstances. We collect, use, and disclose Personal Information concerning our customers for the following reasons:

- To provide timely, reliable, and value-added services to customers including aiding all investigative work conducted;
- To establish a customer relationship and to communicate with customers;
- To develop, implement, market, and manage services for customers;
- To assist in law enforcement purposes, and to protect the business interests of IIS and its customers;
- To manage and promote the business activities of IIS; and
- To meet requirements imposed by law.

We collect, use, and disclose Personal Information concerning our employees for the following reasons:

- To recruit, train, recognize, and retain a highly qualified and motivated workforce;
- To establish and maintain harmonious employer-employee relations;
- To administer IIS policies and procedures, including investigations related thereto;
- To manage and promote the business activities of IIS;
- To administer compensation and benefits;
- To develop, manage, and promote employee services; and
- To meet requirements imposed by law.

If we plan to use Personal Information we have collected for a purpose not previously identified, we will identify and document this purpose before such use. We will make a reasonable effort to specify the identified purposes, orally or in writing, to the individual from whom the Personal Information is collected either at the time of collection or after collection but before use. We will state the identified purposes in such a manner that an individual can reasonably understand how the information will be used or disclosed.

Principle 3 - Consent

Personal Information will only be collected, used, or disclosed with the knowledge and consent of the individual, except where inappropriate.

The way, in which we seek consent, including whether it is express or implied, may vary depending upon the sensitivity of the information and the reasonable expectations of the individual. An individual can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. We will inform individuals of any implications of withdrawing consent.

Typically, we will seek consent for the use or disclosure of information at the time of collection. In certain circumstances, consent may be sought after the information has been collected but before use (such as where we want to use information for a purpose not previously identified).

We will not, as a condition of the supply of services, require an individual to consent to the collection, use, or disclosure of Personal Information beyond that required, to fulfill the explicitly specified and legitimate purposes.

In certain circumstances, as permitted or required by law, we may collect, use or disclose Personal Information without the knowledge or consent of the individual. These circumstances include: Personal Information which is subject to solicitor-client privilege or is publicly available as defined by regulation; where collection or use is clearly in the interests of the individual and consent cannot be obtained in a timely way; to investigate a breach of an agreement or a contravention of a law; to act in respect to an emergency that threatens the life, health or security of an individual; for debt collection; or to comply with a subpoena, warrant or court order.

Principle 4 - Limiting Collection

We will limit the amount and type of Personal Information collected to that which is necessary for our identified purposes and we will only collect Personal Information by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention

Personal Information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal Information will be retained only as long as necessary to fulfill the identified purposes.

Personal Information which has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made and, in the event of an access request or a challenge, long enough to exhaust any recourse an individual may have under the law. Where Personal Information is no longer required to fulfil the identified purposes, it will be destroyed, erased, or made anonymous.

Principle 6 - Accuracy

We will use our best efforts to ensure that Personal Information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

We will use our best efforts to ensure that Personal Information that is used on an ongoing basis, including information that is disclosed to third parties, and information that is used to make a decision about an individual, is accurate, complete, and up-to-date.

Principle 7 - Safeguards

We will protect Personal Information with safeguards appropriate to the sensitivity of the information.

Our safeguards will protect Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which the information is held. We will make our employees aware of the importance of maintaining the confidentiality of Personal Information, and we will exercise care in the disposal or destruction of Personal Information to prevent unauthorized parties from gaining access to the information.

Our methods of protection will include physical measures (for example, locked filing cabinets, alarm and video security systems and restricted access to offices), organizational measures (for example, security clearances and limiting access on a "need-to-know" basis), and technological measures (for example, the use of passwords and encryption).

Principle 8 - Openness

We will make specific information about our policies readily available, except to the extent this is confidential commercial information.

The information we will make available will include: how to gain access to Personal Information; the type of Personal Information held by us, including a general account of its use; general information concerning our Code and policies; what Personal Information is made available to related companies; and how to contact our Chief Information Officer.

Principle 9 - Individual Access

Upon written request, we will inform an individual of the existence, use, and disclosure of his or her Personal Information and we will give the individual access to that Personal Information. An individual can challenge the accuracy and completeness of his or her Personal Information and have it amended as appropriate.

We will respond to an individual's written request within a reasonable time (generally within 30 days). We will assist any individual who informs us that they need assistance in preparing a request. We may require an individual to provide sufficient information to permit us to provide an account of the existence, use, and disclosure of Personal Information. While our response will typically be provided at no cost to the individual, depending on the nature of the request and the amount of information involved, we reserve the right to impose a cost. In these circumstances, we will inform the individual of the approximate cost to provide the response and proceed upon payment by the individual of the cost. Requested information will be provided or made available in a form that is generally understandable. Where possible, we will indicate the source of the information.

In providing an account of third parties to which we may have disclosed Personal Information about an individual, we will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which we have actually disclosed Personal Information, we will provide a list of organizations to which we may have disclosed the information.

If an individual successfully demonstrates the inaccuracy or incompleteness of Personal Information, we will amend the information as required. If a challenge is not resolved to the satisfaction of the individual, we will record the substance of the unresolved challenge. Where appropriate the amended information or the existence of the unresolved challenge, as the case may be, will be transmitted to third parties having access to the information in question.

In certain situations, we may refuse a request or not be able to provide access to all the Personal Information we hold about an individual. Exceptions to the access requirement will be limited and specific, as permitted or required by law. Where permitted, the reasons for denying access will be provided to the individual upon request. Exceptions may include: information that contains references to other individuals or contains confidential commercial information, where such information cannot be severed from the record; information collected in the course of investigating a breach of an agreement or in the course of a formal dispute resolution process; and information that is subject to solicitor-client privilege.

Principle 10 - Challenging Compliance

Any individual can address a challenge concerning our compliance with any of the Privacy Principles to our Chief Information Officer.

We will investigate all written complaints. If we find a complaint to be justified, we will take all appropriate measures, including, if necessary, amending our policies and practices.

For additional information, contact:

Chief Information Officer
Bruce Haines
Independent Investigative Services Inc. (IIS)
(formerly Haines, Miller & Associates Inc.)
290 North Queen Street, Suite 215, Toronto, Ontario. M9C 5L2
Tel: (416) 241-0009 x 25 Fax: (416) 241-9737
Email: bhaines@hainesmiller.com