
Table of Contents

Table of Contents.....	1
Chapter One - Objectives of BP's Privacy Policy	3
1.1 Purpose and Objectives of this Manual.....	3
Chapter Two - Introduction to the Personal Information Protection and Electronic Documents Act and Substantially Similar Provincial Legislation	4
2.1 Purpose of the Privacy laws.....	4
2.2 BP Global Privacy Requirements.....	4
2.3 Status of BP's Suppliers, Customers, and Business Partners Under BP's Privacy Policy	4
2.4 What Does BP's Privacy Policy Mean to Me?.....	4
2.5 To Obtain More Information About PIPEDA, SSPL and BP's Privacy Policy.....	5
Chapter Three - Collection of Personal Information By BP	6
3.1 Collection of Personal Information	6
3.2 Purposes for Collecting Personal Information.....	6
3.3 Criteria Used to Determine Whether Personal Information Should Be Collected	7
3.4 Manner In Which Personal Information Is Collected	7
Chapter Four - Use and Disclosure of Personal Information	11
4.1 Use of Personal Information	11
4.2 Disclosure of Personal Information	11
4.3 Obtaining Consent.....	13
4.4 Revoking or Modifying Consent	14
Chapter 5 - Retention of Personal Information.....	15
5.1 Retention Rules.....	15
Chapter 6 - Protection of Personal Information.....	16
6.1 Protection Measures.....	16
6.2 Security Breaches.....	16
6.3 Common Protection Rules.....	17
Chapter 7 - Disposal of Personal Information	18
7.1 Destruction of Physical Media:.....	18
7.2 Destroying Electronic Information:.....	18
Chapter 8 - Individuals' Right of Access to His or Her Personal Information and His or Her Right to Request Its Correction	19
8.1 Rights of An Individual to Have Access to His or Her Personal Information Under the Control of BP	19
8.2 Does an Individual Have to Invoke the BP Privacy Policy to Gain Access to His or Her Personal Information?	19
8.3 Procedure to Request Access to Personal Information Under the Privacy Laws	19
8.4 Fees to Request Access to Personal Information	20
8.5 Time Limits For Responding to Request for Personal Information.....	21
8.6 Refusal to Grant Access to Sensitive Personal Information.....	21
8.7 Where the Requested Information Cannot Be Identified or Retrieved	22
8.8 Procedure for the Processing of Formal Access Requests.....	22

8.9	Procedure for the Processing of Requests for the Correction of Personal Information	24
Chapter 9	Structure of BP's Privacy Program	26
9.1	The Need for a Privacy Coordinator	26
9.2	Role of the Privacy Coordinator	26
9.3	Obligation to Inform the Privacy Coordinator	26
9.4	Complaints	27
9.5	Audits	28
Appendix 1	Personal Information Request Form	29
Appendix 2	Personal Information Correction Request Form	30
Appendix 3	Privacy Impact Assessment (PIA) Guide - Short Version	31
Appendix 4	Contacts	33
4.1	Internal Contacts at BP	33
4.2	To Obtain a Copy of BP's Privacy Policy	33
4.3	To Obtain a Copy of the Privacy Acts That Are Currently In Effect:	33

Chapter One - Objectives of BP's Privacy Policy

1.1 Purpose and Objectives of this Manual

BP Canada Energy Company and its affiliates (hereinafter called "BP") support the principles set forth in the Personal Information Protection and Electronic Documents Act (PIPEDA) and substantially similar provincial legislation (SSPL). We believe that the objectives are consistent with our business objectives and that compliance with them will further our business as it relates to ethics; employee relations; community and customer relations; health, safety and environmental performance; and control and finance.

This manual describes the requirements and detailed procedures that we have established to ensure that BP can fulfill its obligations under PIPEDA and SSPL.

This policy and its related procedures seek to:

- a) Facilitate compliance with the objectives of the applicable privacy laws and codes in each jurisdiction where we operate;
- b) Ensure that privacy protection is fully integrated into all administrative and operational processes at BP and does not add an unreasonable burden on our resources;
- c) Ensure that we can adequately respond to any questions about our projects, policies, programs, systems and practices that involve the use of personal information;
- d) Allow us to promptly address any concerns that may be expressed by our customers, vendors or suppliers, employees, business partners or by the Privacy Commissioner of Canada or the appropriate provincial Privacy Commissioner in relation to the management of the personal information under our control;
- e) To stress the importance of incorporating the requirements of the privacy laws into BP's plans and objectives and to think "privacy" at the beginning of the planning phase of all projects;
- f) Provide a framework to ensure that all privacy reviews and Privacy Impact Assessments (PIA) are conducted in a consistent manner; and
- g) Facilitate the dissemination of information about the privacy laws to all our managers, employees, contractors, suppliers and business partners.

Chapter Two - Introduction to the Personal Information Protection and Electronic Documents Act and Substantially Similar Provincial Legislation

2.1 Purpose of the Privacy laws

PIPEDA and SSPL aim to give individuals more control over their personal information by limiting the right of privately owned companies that collect, use and disseminate personal information in the course of commercial activities. In addition, they grant individuals the right to request access to most of the personal information about them that is kept by those organizations and the right to request the correction of that personal information.

2.2 BP Global Privacy Requirements

BP P.L.C. has global privacy requirements that BP will comply with through its privacy policy.

2.3 Status of BP's Suppliers, Customers, and Business Partners Under BP's Privacy Policy

Even though all commercial companies in Canada are now subject to some form of privacy legislation (either PIPEDA or SSPL), it is important to mention that all suppliers and business partners who collect or use personal information in the course of their duties for BP are subject to BP's privacy policy.

2.4 What Does BP's Privacy Policy Mean to Me?

All managers, employees, suppliers, and business partners of BP must adhere to the requirements of BP's privacy policy. In line with the policy, they must limit the collection of personal information about other individuals to only what they need to conduct their business on behalf of the company. They cannot use, disclose, exchange, share, or dispose of that personal information in a way that is contrary to the policy.

Under BP's privacy policy, every individual may request access to his or her personal information that is kept by BP, our suppliers, or our business partners. An individual who believes that his or her personal information is incomplete or inaccurate may also request the correction of that personal information. Access to an individual's own personal information may be denied or restricted under some circumstances, and the correction of the personal information may be denied if the individual cannot substantiate his or her claim that the information is incomplete or inaccurate. Because evaluative information or

subjective comments cannot be corrected, the company will not grant requests for the correction of such information. BP will instead annotate the information to show any disagreement expressed by an individual in relation to the comments in the document.

2.5 To Obtain More Information About PIPEDA, SSPL and BP's Privacy Policy

You can contact BP's Privacy Coordinator by:

Internal	External
email: bpcanadaprivacycoordinator@bp.com	email: bpcanadaprivacycoordinator@bp.com
Phone: <ul style="list-style-type: none"> • In Calgary – 233-1634 • Local 1634 	Phone: <ul style="list-style-type: none"> • 1 -877-232-1634
	Traditional mail:
	Attention: BP Canada Privacy Coordinator BP Canada Energy Company 240 – 4 Avenue SW P.O. Box 200 Calgary, AB T2P 2H8

Chapter Three - Collection of Personal Information By BP

3.1 Collection of Personal Information

The expression "collection of personal information" refers to the acquisition of new knowledge about an identifiable individual. This knowledge can be acquired in several ways, including questionnaires to be completed by candidates for employment, by individuals who apply for benefits or by those who participate in customer or employee satisfaction surveys; through public opinion polls; by consulting participants/ mailing lists; through an internal investigation; etc. Regardless of what method is used to obtain the personal information, it is considered a "collection".

3.2 Purposes for Collecting Personal Information

Because of the nature of its business, BP does not collect significant amounts of personal information. Most of the personal information that the company collects pertains to our own employees, our individual contractors or customers and our individual business partners. Most of that personal information is used in the management of the pay/benefits programs of the company or for the management of the contracting and procurement processes. More specifically, BP collects personal information for the following purposes:

a) To comply with legal and regulatory requirements:

These requirements include the collection and the creation of files and information about individuals in accordance with the Income Tax Act, workers' compensation legislation and other privacy laws and regulations that require reporting to government agencies.

b) To support the effective management of human resources:

This encompasses the management of our human resources, including functions such as recruiting, the MyPerformance process, learning and development activities, relocation of employees and the administration of the compensation/benefits package that we offer. The information is also used to produce management reports.

c) To ensure the adequate protection of employee and BP's information and assets:

BP collects personal information that directly relates to, and is necessary for the achievement of our safety and environmental performance objectives and to ensure the safe and secure extraction, processing and distribution of our products while meeting environmental, legal and regulatory requirements. These objectives include health and safety, the administration of the drug and alcohol policy, accident

prevention and reporting, emergency response, business resumption planning and measures that ensure the protection of BP's information and assets.

d) To serve our customers and further BP's business objectives:

This section covers the effective and efficient extraction, processing and distribution of our products while meeting legal, regulatory and contractual requirements; the conduct of business and financial transactions; and effective communications with our shareholders and business partners.

3.3 Criteria Used to Determine Whether Personal Information Should Be Collected

There are three important factors to consider in making this determination:

- a) Personal information that would fall into the "nice to know" category but which is not necessary for the achievement of BP's business objectives must not be collected;
- b) Only those employees who need the personal information to perform their duties are allowed to collect or access it;
- c) The limitation on the amount of personal information collected also reduces the costs associated with the retention, maintenance and protection of that personal information.

To ensure compliance with the above objectives, each business or functional unit of BP that collects a new category of personal information must, prior to collecting the information, conduct a Privacy Impact Assessment ("PIA"). The specific conditions for the conduct of PIAs and the details of the PIA process are provided in a later chapter. The Privacy Coordinator can also provide additional information.

3.4 Manner In Which Personal Information Is Collected

a) Purpose of the Collection:

The privacy laws require that wherever possible, the individual must be informed of the purpose of the collection. In line with the spirit of this requirement, we will, whenever possible and legally permitted, inform the individual about whom personal information is being collected, of the following aspects of the collection and the subsequent treatment of the personal information:

- i) The specific business purpose for the collection;
- ii) Where applicable, the legal or other authority under which the information is collected;

-
- iii) Whether the individual is under the obligation to provide the information to BP and, where applicable, the consequences of any refusal to provide it;
 - iv) BP's records retention code to which the personal information is associated (that code can be found by consulting the BP Affiliated North American Companies' Records Retention Schedule (hereafter "BP's Retention Schedule));
 - v) The identity of the groups within BP and the identity of outside groups who will be given access to the information and the reason for the disclosure;
 - vi) A list of the uses and consistent uses* that BP will make of the information.

*Note: A "consistent use" is the use of personal information in a decision making process that has a direct and logical link with the process for which it was initially collected. A good example would be the use of a MyPerformance form as an evaluation instrument for a staffing process. While the performance report was not prepared specifically for the purpose for which it is being used, the fact that both processes seek to assess the strengths and areas of improvement for the employee in relation to a work related situation makes the use of the performance form in the staffing process a "consistent use".

- vii) The records retention period.

Although this information may be provided verbally to an individual, BP's preferred approach is to document the process and retain a record of it. The best method is to include a short Privacy Statement on the questionnaire, the application form or the medical report form that is used for the collection of the personal information. The privacy statement can also be provided through an information pamphlet or brochure given to all individuals from whom personal information is collected. The following text can be used as a model for the preparation of Privacy Statements:

"The personal information collected via this form is associated with BP's Retention Code number ZZZZZ and will be used and handled in accordance with the description provided in the Personal Information Directory located at (<http://canada.bpweb.bp.com/hr/privacy>)."

Notes:

Contractors and business partners of BP must inform the individuals from whom they collect personal information that they are acting on behalf of BP. They must also provide the same information about the collection as BP would provide if the information was collected directly by BP;

BP employees, contractors and business partners cannot promise confidentiality when collecting personal information, and cannot act in any manner that may suggest that the information collected will be protected from access under the privacy or other laws.

b) Direct Collection Principle:

The privacy laws impose an obligation to:

- i) Obtain consent from an individual before collecting personal information about him or her whenever possible; and
- ii) Collect that information directly from the individual except if the individual consents to the collection of that information from another source.
- iii) The exceptions to the direct collection principle include:
 - iv) Where legal, medical or security reasons make it impossible or impractical to seek consent;
 - v) Where information is being collected for the detection and prevention of fraud or for law enforcement, and seeking consent might defeat the purpose of collecting the information;
 - vi) Where seeking consent is impossible or inappropriate because the individual is a minor, seriously ill, or mentally incapacitated;
 - vii) Where the company does not have a direct relationship with the individual and may not always be able to seek consent;
 - viii) Where the direct collection would likely produce inaccurate information, such as when the information is obtained in the course of an investigation.

c) Indirect Collection:

The following list of questions, which is not exhaustive, can help determine if indirect collection is appropriate in a given situation:

- i) How would informing the individual that personal information about him or her is being or will be collected:
 - aa) Affect the immediate or future use of the information?
 - bb) Result in the collection of inaccurate information?
- ii) How would getting consent or informing the individual of the purpose of the collection of personal information about him or her:

- aa) Affect the immediate or future use of the information?
- bb) Result in the collection of inaccurate information?
- iii) What serious consequences would likely occur if the individual were told about the collection of the personal information? Would these consequences be serious (i.e., the safety of another individual might be at risk or there could be serious repercussions for BP's programs) or would they just cause administrative inconvenience?

Chapter Four - Use and Disclosure of Personal Information

4.1 Use of Personal Information

Normally, personal information is used to make the following types of decisions:

- a) Administrative (e.g., for the management of human resources);
- b) Operational (e.g., for the management of BP's business processes);
- c) Judicial (e.g., for use in court);
- d) Quasi-judicial (e.g., for use in a legal process before an administrative tribunal as opposed to before a court of law).

The privacy laws provide that personal information may only be used for the following four purposes:

- a) The purpose for which the personal information was initially collected;
- b) A use that has a direct and logical link with the original use – known as a “consistent use”;
- c) A use for one of the special circumstances that are specified in the privacy laws, such as law enforcement purposes, emergency situations, research, etc. where the personal information of an individual can be used without the knowledge or consent of that individual;
- d) Any other use for which the individual has given informed consent.

All uses and consistent uses are listed in BP's Personal Information Directory, therefore, you should consult this publication before using personal information for a new or an unconventional use. When in doubt about the legitimacy of the new use, you should contact the Privacy Coordinator.

4.2 Disclosure of Personal Information

Allowing another person or party to acquire the knowledge that we possess about an individual constitutes a “disclosure of personal information”. In accordance with the privacy laws, BP can disclose personal information under certain circumstances. Those circumstances vary from province to province, but here are some examples of the ones that we are likely to find in most privacy laws:

- a) Disclosure with the consent of the individual to whom the information relates. This provision is often used by employees who sign a letter of consent to allow their

spouse to perform certain transactions on their behalf. The responsibility of BP's representatives in such a situation is to satisfy themselves that:

- i) the signature on the letter of consent is really the signature of the employee;
 - ii) the individual who claims to be the appointed representative of another person is the legitimate representative of that person; and
 - iii) the disclosure of the personal information would not cause any harm to the individual who has consented to the disclosure or to another person.
- b) Disclosure for the purposes for which the personal information was collected or for a purpose that is consistent with that intended purpose (consent from the individual to whom the information pertains is not necessary in this case);
- c) Disclosure in accordance with an Act or a regulation (consent from the individual to whom the information pertains is not necessary in this case);
- d) Disclosure, without the knowledge or consent of the individual to whom the personal information relates, under any of the other special circumstances listed in the privacy laws. Again, those circumstances vary from province to province, but they generally include the following:
- i) if the disclosure is made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the corporation;
 - ii) for the purpose of collecting a debt owed by the individual to the organization;
 - iii) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
 - iv) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that:
 - aa) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
 - bb) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
 - cc) the disclosure is requested for the purpose of administering any law of Canada or a province;

- d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization
 - i. has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
 - ii. suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
- e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;
- f) for statistical, or scholarly study or research purposes that cannot be achieved without disclosing the information and it is impracticable to obtain consent and the organization informs the appropriate Privacy Commissioner of the disclosure before the information is disclosed;
- g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;
- h) made after the earlier of
 - i) one hundred years after the record containing the information was created, and
 - ii) twenty years after the death of the individual whom the information is about;or
 - iii) required by law.

4.3 Obtaining Consent

- a) The consent of an individual to have his or her personal information disclosed to another party must be obtained in accordance with the following requirements:
- b) The individual must be given an opportunity to identify the personal information to be disclosed. This can be done either by providing the individual with a copy of the information or by inviting the individual to review the information in a BP office;
- c) The individual must be informed of all the reasons for the disclosure;
- d) We must clearly identify all the parties to whom the information will be disclosed, and we must provide a description of the information that will be disclosed to each party;

- e) The individual must be informed that he or she can impose certain limitations on the disclosure of the information with respect to:
 - i) The exact nature and amount of information that will be disclosed to each party;
 - ii) The length of time for which consent is given - consent shall not usually be considered as permanent except where the information is collected for the long-term management of a program (such as employee benefits) or it is specified in the consent form or letter signed by the individual;
- f) The individual must be informed of the potential consequences that may result from the disclosure, to the extent that those consequences are known to BP;
- g) Should BP ever discover at a later date that unexpected consequences have resulted from the disclosure of the individual's personal information, it may consider informing the individual of the situation;
- h) The individual must be informed of the possible consequences that could result from his or her refusal to consent to the disclosure;

Notes:

- BP cannot assume that the individual who is asked or offered to provide consent for the disclosure of his or her personal information appreciates the consequences of his or her decision. BP representatives who contact an individual to obtain consent must make a reasonable effort to ensure that the individual fully understands the implications of his or her decision in that respect;
- Where appropriate, BP should consider offering the individual the opportunity to disclose the information himself or herself.

4.4 Revoking or Modifying Consent

An individual may at any time withdraw or vary consent to the collection, use or disclosure of personal information by the company by giving reasonable notice and, upon receipt of a notice, BP must:

- a) Inform the individual of the consequences of his or her decision; and
- b) Stop the collection, use and disclosure as instructed by the individual unless the law states otherwise.

Chapter 5 - Retention of Personal Information

5.1 Retention Rules

Two rules apply to the retention of personal information:

- a) Personal information must be retained only as long as necessary for the fulfillment of the purposes for which it was collected; and
- b) Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

Under normal circumstances, one year is considered the shortest length of time personal information should be retained. BP Affiliated North American Companies' Records Retention Schedule specifies the length of time for which each broad category of records of the company must be kept, and everyone within the company is expected to adhere to those requirements.

Except where provided for by the privacy laws, this policy or by BP Affiliated North American Companies' Records Retention Schedule, records that contain personal information must not be destroyed:

- a) Contrary to any Act or regulation;
- b) To avoid embarrassment for BP Affiliated North American Companies' or for one of its managers or employees;
- c) If the information is involved in a complaint, appeal, litigation or another judicial or quasi-judicial process;
- d) If the information is involved in, or is required for law enforcement purposes;
- e) If the disposal could affect the business interests or the reputation of BP.

Note:

BP must not retain paper or electronic copies of the personal information that it created or used in excess of the period for which it is needed. If a copy of a document is kept to use as a template, it must be depersonalized before saving.

Chapter 6 - Protection of Personal Information

6.1 Protection Measures

The protection of personal information is ensured through the following mechanisms:

- a) The implementation of physical barriers to control access to the sites and containers where personal information of a sensitive nature is being kept;
- b) The establishment of electronic mechanisms in accordance with the Group Security policies to control, monitor and limit access to electronic information;
- c) The implementation of policies and procedures to ensure the secure treatment of the personal information that is in the custody or under the control of the company;

6.2 Security Breaches

Security breaches may jeopardize the safety of individuals and adversely affect the company's reputation. As a result, the company has implemented measures to prevent their occurrence and respond to security incidents when they do occur. These measures include:

- a) An obligation for all employees to report immediately any security breach or violation that involves personal information to the Privacy Coordinator, the BP Canada Corporate Security group and, where the breach involves electronic information, the Digital Communications & Technology Site Operations Manager;
- b) An obligation for all employees to cooperate in the investigation of security breaches;
- c) The establishment of an emergency response plan that provides for a quick response to any kind of threat that may affect personal information, especially where the threat may have serious consequences for the individuals to whom the personal information pertains;
- d) Identifying the requirement to assess the need to inform the individuals whose personal information has been compromised, of the situation and to offer them assistance in protecting themselves against the consequences of the breach or violation;
- e) The creation of a log to document the circumstances of all security breaches or violations that involve personal information, and to document the measures that are taken in response to each security breach or violation.

Generally, personal information is considered "particularly sensitive" and must be treated in a manner that is consistent with that designation. This involves using approved containers to store and transport it, as well as ensuring that the computer systems that are used to manipulate it are configured in a way that offers reasonable protection against unauthorized access.

6.3 Common Protection Rules

Requests for personal information regarding employees or customers should be referred to Human Resources.

Chapter 7 - Disposal of Personal Information

7.1 Destruction of Physical Media:

Paper and electronic records, as well as all other media that contain personal information must not be disposed of in recycling or garbage bins. These records must be shredded or destroyed in a manner approved by the company, as stated in the Group Security Policy.

7.2 Destroying Electronic Information:

It must also be noted that erasing or reformatting a diskette or a hard drive using the conventional methods in DOS or Windows does not destroy the information. It only erases the electronic index that allows for the retrieval of the information by the computer. Software available on the market may recreate the index in a matter of minutes. If in doubt about BP's approved methods of erasing information from any electronic media, please seek assistance from Digital Communications & Technology Site Operations Manager.

Chapter 8 - Individuals' Right of Access to His or Her Personal Information and His or Her Right to Request Its Correction

8.1 Rights of an Individual to Have Access to His or Her Personal Information Under the Control of BP

Every individual has the right to request access to personal information about himself or herself that is kept by BP. However, the privacy laws do not guarantee that BP will grant access to all of the requested information. In accordance with the privacy laws, BP may refuse access to personal information where the disclosure of that information could, for example, adversely affect the privacy rights of other individuals, the business interests of the company, the conduct of law enforcement activities or any of the other interests that are protected by the privacy laws. The reasons for refusing access are discussed later in this chapter.

8.2 Does an Individual Have to Invoke the BP Privacy Policy to Gain Access to His or Her Personal Information?

No! Individuals who are seeking access to BP's records are encouraged to use the informal mechanisms used historically within BP prior to resorting to the processes under the privacy laws. Employees can request access to their personal information through their immediate team leader or by contacting Human Resources. Informal mechanisms include requesting the information by telephone, in person or in writing without invoking the privacy laws. The benefits of the informal approach include a simpler and faster process; lower costs for all parties; and a less legalistic way to resolve access related issues.

Whether the requester uses the informal process or invokes the privacy laws, he or she will not be allowed access to information that qualifies for an exception to the right of access under the privacy laws. For this reason, it is important that all records to which access is sought be carefully reviewed by their custodian and that any information that may qualify for an exception be removed from them before access is granted. Where applicable, the individual must also be informed that some of the information contained in a document has been removed. In cases where the majority of the information requested is identified as potentially subject to an exception, the individual must be asked to apply under the privacy laws.

8.3 Procedure to Request Access to Personal Information under the Privacy Laws

The following procedure has been established in accordance with the privacy laws, but individuals who are seeking access to BP's records are encouraged to use the informal

mechanisms before resorting to the processes under the privacy laws. Using the privacy laws implies a more "formal" process as the request must meet certain requirements and must be responded to in writing by BP within thirty days (under normal circumstances). In addition, the individual who uses the privacy laws to request access to his or her personal information may lodge a complaint with the federal or provincial Privacy Commissioner (whichever has jurisdiction) if he or she is not satisfied with the response (or the lack of response) from BP. Again, an informal request is, in most cases, the fastest and the cheapest way to access one's own personal information as the information may be disclosed almost immediately to the requester.

- a) A formal request can be made on the "Personal Information Request Form" in Appendix 1;
- b) Formal access requests must be sent to the Privacy Coordinator of the company and provide the following information:
 - i) specify the nature of the personal information requested;
 - ii) where possible, provide an indication as to where the personal information may be held or by whom it may be kept;
 - iii) the identity and mailing address of the requester;
 - iv) a telephone number where the requester may be reached during normal business hours;
 - v) it must be signed and dated.

8.4 Fees to Request Access to Personal Information

The privacy laws provide that organizations can charge a reasonable fee for responding to access requests, however, in line with BP's openness policy, we would normally only charge a fee in the following circumstances:

- a) The cost of providing access is significant, where the request is for a large number of records or one which necessitates a search through a large number of records;
- b) The processing of the access requests interferes with the operations of the company, such as where the individual asks that the information be provided within a short time frame in order for him or her to meet a deadline;
- c) The individual has requested that the information be provided in an irregular format for special reasons, such as when it is required by a government agency or for court purposes;

- d) The request is of a repetitive nature, which can be the case where the individual has been provided with the same information within the last few months; or
- e) The request is unreasonable, such as where it is clear that the request only seeks to disrupt the operations of the company or that it is presented as a way to express dissatisfaction with the company's rules or business practices.

8.5 Time Limits for Responding to Request for Personal Information

Under normal circumstances, the Privacy Coordinator will respond to an access request within thirty calendar days from the date of its receipt. This time limit can be extended where consultations with an outside party are required or where special circumstances make it impossible for BP to meet the time limit. Where the time limit is extended, the Privacy Coordinator will inform the requester of the reason for the extension and of the date by which the response will most likely be sent.

8.6 Refusal to Grant Access to Sensitive Personal Information

The privacy laws contain a number of exception provisions that provide for the refusal of access to certain categories of personal information. Although these exceptions vary from province to province and are usually determined by the Privacy Coordinator, the following list provides examples of the kinds of information that may be subject to them:

- a) the information is protected by solicitor-client privilege;
- b) the disclosure of the information would reveal confidential commercial information;
- c) the disclosure of the information could reasonably be expected to threaten the life or security of another individual;
- d) the information pertains to an investigation into a breach of an agreement or a contravention of the laws of Canada or a province by a law enforcement agency; or
- e) the information was generated in the course of a formal dispute resolution process.

Even though BP is allowed to refuse to disclose the portions of a record that could reveal confidential commercial information or that could reasonably be expected to threaten the life or security of another individual, the company will still provide access to as much of the remaining information as possible.

8.7 Where the Requested Information Cannot Be Identified or Retrieved

The letter of response from the Privacy Coordinator will inform the requester of the results of the search for the information. The letter will also indicate that the requester has a right to complain to the Privacy Commissioner of Canada.

8.8 Procedure for the Processing of Formal Access Requests

- a) An individual who wishes to request access to his or her personal information should use the Personal Information Request Form in Appendix 1;
- b) Upon receipt of the access request, the Privacy Coordinator will stamp the request to show its date of receipt;
- c) Where applicable, the Privacy Coordinator will confirm the legitimacy of the request (proper authorization to release to third party, confirm all parties involved in the documentation have signed the request, the individual has the right to request under the applicable privacy legislation, etc.);
- d) If necessary, the Privacy Coordinator will contact the individual to clarify the nature and the scope of the access request or to obtain more information about the personal information being sought by the requester;
- e) The Privacy Coordinator will then:
 - i) Assign a file number to the request;
 - ii) Send a confirmation of receipt of request to the individual;
 - iii) Start a BP activity log to record discussions, actions, communications, correspondence, etc.;
 - iv) Start a tracking document;
- f) Where the access request cannot be responded to within the thirty-day time limit, the Privacy Coordinator will send a notice to the requester specifying the following information:
 - i) The reason for the extension; and
 - ii) The date by which the response will be sent.
- g) The Privacy Coordinator requests by e-mail or by fax the relevant files and documentation from all areas of BP. The covering note will specify the date by which

- the files or documentation must be sent to his or her office by the custodians of the information;
- h) The Privacy Coordinator consults with file personnel for information relevant to the processing of the request and recognizing limitations under the applicable privacy law (refer to fees);
 - i) The Privacy Coordinator sends the notice of applicable fee (where appropriate) associated with the processing of the access request to the requester. The notice shall require payment of at least 50 % of the total fee before the access request is processed;
 - j) The Privacy Coordinator photocopies and numbers all copies of the records to be processed for the purpose of the access request;
 - k) Where appropriate, the Privacy Coordinator sends the documentation requiring third party consultation by courier or by registered mail to the third party with a cover letter of explanation and include the sections of the applicable privacy law pertinent to the request. The letter will specify the date by which the response of the third party must be received by the Privacy Coordinator;
 - l) The Privacy Coordinator determines the exceptions to the records in accordance with the applicable privacy legislation;
 - m) Once information is removed from the documents (words, paragraphs or complete pages, etc.) the Privacy Coordinator makes a photocopy so that it may be viewed by or provided to the requester;
 - n) The Privacy Coordinator prepares a cover letter for the requester outlining the sections of the applicable privacy legislation used to withhold any information not being provided to requester;
 - o) The Privacy Coordinator collects any outstanding fees (if applicable) associated with the processing of the access request;
 - p) If the requester wishes to view the documents rather than be provided with copies, the Privacy Coordinator books a reading room and informs the requester of the arrangements;
 - q) The Privacy Coordinator returns original documents to their areas of origin;
 - r) The Privacy Coordinator closes the file.

8.9 Procedure for the Processing of Requests for the Correction of Personal Information

- a) Individuals who wish to request the correction of their personal information should use the Personal Information Correction Request Form in Appendix 2;
- b) Upon receipt of the access request, the Privacy Coordinator will stamp the request to show its date of receipt;
- c) Where applicable, the Privacy Coordinator will confirm the legitimacy of the request (proper authorization to release to third party, have all parties involved in the documentation signed the request, the individual has the right to request under the privacy laws, etc.);
- d) If necessary, the Privacy Coordinator will contact the individual to clarify the nature and the scope of the correction request;
- e) The Privacy Coordinator will then:
 - i) Assign a file number to the request;
 - ii) Send a confirmation of receipt of request to the individual;
 - iii) Start a BP activity log to record discussions, actions, communications, correspondence, etc.;
 - iv) Start a tracking document;
- f) Where the correction request cannot be responded to within the thirty-day time limit, the Privacy Coordinator will send a notice to the requester specifying the following information:
 - i) The reason for the extension; and
 - ii) The date by which the response will be sent.
- g) The Privacy Coordinator requests by e-mail or by fax the relevant files and documentation from all areas of BP. The covering note will specify the date by which the files or documentation must be sent to his or her office by their custodians;
- h) The Privacy Coordinator consults with file personnel to determine whether the request can be granted and recognizing limitations under the applicable privacy law (i.e. where the corrections refer to subjective or evaluative material);
- i) Where appropriate, the Privacy Coordinator sends the documentation requiring third party consultation by courier or by registered mail to the third party with a cover letter of

explanation and include the sections of the applicable privacy law pertinent to the request. The letter will specify the date by which the response of the third party must be received by the Privacy Coordinator;

- j) The Privacy Coordinator decides to make the requested corrections and document all files appropriately. Where the corrections are granted, the records that contained the original information must be cross-referenced to indicate that their content has been amended by another record. The original records will not normally be destroyed, as this could deprive BP of a defence in case of litigation;
- k) Once the corrections have been made, the Privacy Coordinator makes a copy of the amended records to the requester;

The Privacy Coordinator prepares a cover letter for the requester explaining the decision in relation to the requested corrections and sends the letter with the copies of the amended records to the requester;

- l) The Privacy Coordinator returns original documents to their areas of origin;
- m) The Privacy Coordinator closes the file.

Chapter 9 - Structure of BP's Privacy Program

9.1 The Need for a Privacy Coordinator

The privacy legislation requires the designation of a person who will coordinate all privacy related activities within the company and be accountable for BP's compliance with the applicable privacy legislation. The designated person for BP Canada is the BP Canada Privacy Coordinator.

9.2 Role of the Privacy Coordinator

The role of the Privacy Coordinator includes:

- a) Developing policies and procedures for the orderly implementation of the privacy legislation;
- b) Promoting awareness of the legislation to ensure compliance at BP;
- c) Processing formal requests for access to personal information from individuals, and advising senior management of the disposition of these requests;
- d) Monitoring BP's compliance with the applicable privacy legislation and with all regulations, policies and procedures that govern the management of personal information by BP;
- e) Providing guidelines for, and assisting managers and employees in the conduct of Privacy Impact Assessments (PIA);
- f) Responding to complaints made by individuals in relation to the management of his or her personal information or to his or her right of access to it;
- g) Acting as spokesperson for BP in dealings with the applicable Office of the Privacy Commissioner and with other government departments and agencies on privacy matters.

9.3 Obligation to Inform the Privacy Coordinator

Many projects that involve the collection, use and disclosure of personal information have an impact on the privacy rights of individuals. As a result, it is essential to involve the Privacy Coordinator as early as possible in the decision making process that pertains to those projects. The involvement of the Privacy Coordinator presents the following advantages:

- a) It may prevent BP from investing resources in projects that may not meet the requirements of the applicable privacy legislation or pass the "privacy test";
- b) It may prevent BP from entering into agreements that involve the collection, use or disclosure of personal information contrary to the applicable privacy legislation or this policy;
- c) It ensures that a proper Privacy Impact Assessment (PIA) is conducted in relation to that project;
- d) It may avoid redundancy by preventing the conduct of a PIA for a program or project that has been the subject of a previous PIA;
- e) It allows the Privacy Coordinator to make suggestions in relation to the design of the project and in relation to the manner in which the PIA should be conducted;
- f) It provides for an opportunity to address all BP policy and privacy related requirements during the course of the PIA.

A guide for the conduct of Privacy Impact Assessments is provided in Appendix 3.

9.4 Complaints

Complaints regarding the implementation of privacy legislation or of this policy should normally be made in writing or by email to the Privacy Coordinator. Upon receipt of a complaint, the Privacy Coordinator will:

- a) Contact the individual to clarify the reasons for the complaint;
- b) Investigate the issue by collecting all relevant information;
- c) Where appropriate, mediate resolution of the complaint with the individual;
- d) Where the complaint is justified in whole or in part, the Privacy Coordinator shall immediately take every reasonable step to resolve the issue;
- e) Inform the individual of the results of the complaint and, where appropriate, of any action taken to resolve the issue.

9.5 Audits

The Privacy Coordinator may occasionally conduct privacy compliance audits as a way to assess BP's compliance with the objectives of the applicable privacy legislation. The following circumstances may bring the Privacy Coordinator to conduct an audit:

- a) Following a complaint about a systemic issue regarding the applicable privacy legislation;
- b) At the suggestion of the Privacy Commissioner of Canada or the Privacy Commissioner of a province;
- c) Upon the recommendation from the BP Canada Corporate Security group;
- d) At the request of Human Resources, or at the request of the manager of a functional unit;
- e) As a result of a threat and risk assessment;
- f) For any other reason which, in the opinion of the Privacy Coordinator, requires the conduct of an audit.

To ensure a more consistent approach and prevent any interference with a possible ongoing security investigation, privacy compliance audits will normally be conducted in cooperation with the BP Canada Corporate Security group.

Appendix 1 - Personal Information Request Form

Request Number: (For Office Use Only)

	IDENTITY OF REQUESTER
SURNAME:	
GIVEN NAME:	
ADDRESS:	
TELEPHONE NUMBER:	
FAX NUMBER:	
EMAIL ADDRESS:	

DESCRIPTION OF RECORDS SOUGHT: (Please consult BP's Personal Information Directory to identify the applicable Retention Code for the information to which you are seeking access)

Signature: _____

Dated: _____

Appendix 2 - Personal Information Correction Request Form

Request Number: (For Office Use Only)

	IDENTITY OF REQUESTER
SURNAME:	
GIVEN NAME:	
ADDRESS:	
TELEPHONE NUMBER:	
FAX NUMBER:	
EMAIL ADDRESS:	

DESCRIPTION OF CORRECTIONS SOUGHT: (Please consult BP's Personal Information Directory to identify the applicable Retention Code for the information you want corrected. Attach additional sheets to this form if necessary)

SUPPORTING INFORMATION:

Supporting proof/information for the corrections is enclosed:

Supporting proof/information for the corrections is not enclosed but can be obtained from the following source(s):

--

Signature: _____

Dated: _____

Appendix 3 - Privacy Impact Assessment (PIA) Guide - Short Version

Note:

At the beginning of all projects an analysis needs to be conducted to determine if any personal information will be collected, used or disclosed as a result of the project.

The short version of the PIA Guide can be used for most of the PIAs that need to be conducted in relation to new business activities, programs and systems (projects) that are locally established. The comprehensive version of the PIA Guide, which is more suitable for company-wide projects, can be obtained from BP Canada Privacy Coordinator.

Upon completion of the PIA Guide, please contact the BP Canada Privacy Coordinator for further review and assistance.

PIA GUIDE

The purpose of this grid is to have the PIA team describe as precisely and objectively as possible the nature of the personal information that will be involved in the project, program, or system to be examined and the context in which that personal information will be collected, used, disclosed, stored and protected. It is the first step in the systematic review of the sensitivity of the personal information.

	Criteria or Technical reference	Descriptions and Details
1	Provide a general description of the most important categories of personal information that will be used by the program or system.	
2	Provide the authority or the rationale for the collection of the personal information and explain why the program or system could not meet its objective without the personal information.	
3	Describe the intended and the real uses that are being made of the personal information.	
4	Describe the intended and real disclosures of the personal information.	
5	List the agreements that may exist in relation to that personal information. Attach a copy of the confidentiality, privacy and security clauses that may exist in those agreements.	
6	List the statutory, regulatory or policy requirements for the confidentiality of the personal information.	
7	Provide the following details in relation to the retention and disposal schedule established for the personal information: a) How long is the personal information kept by the company or by any other party who will have access to it? Is this in accordance with the BP Affiliated North American Companies' Records Retention Schedule? b) Describe how the personal information (paper, electronic and other media) will be disposed of at the end of its life cycle.	

Appendix 4 - Contacts

4.1 Internal Contacts at BP

Individuals who have questions about the implementation of the PIPED Act, a SSPL or about the BP Canada Privacy Policy and procedures may contact the BP Canada Privacy Coordinator by:

Internal	External
email: bpcanadaprivacycoordinator@bp.com	email: bpcanadaprivacycoordinator@bp.com
Phone: <ul style="list-style-type: none">• In Calgary 233-1634• Local 1634	Phone: <ul style="list-style-type: none">• 1-877-232-1634
	Traditional mail:
	Attention: BP Canada Privacy Coordinator BP Canada Energy Company 240 – 4 Avenue SW P.O. Box 200 Calgary, AB T2P 2H8

4.2 To Obtain a Copy of BP's Privacy Policy

BP's privacy policy is available at the following Internet address:

URL: <http://canada.bpweb.bp.com/hr/privacy>

4.3 To Obtain a Copy of the Privacy Acts That Are Currently In Effect:

Alberta: <http://www.psp.gov.ab.ca/legislation/index.html>

British Columbia: http://www.legis.gov.bc.ca/37th4th/3rd_read/gov38-3.htm

Federal (PIPEDA): <http://laws.justice.gc.ca/en/P-8.6/91100.html>

Quebec: <http://doc.gouv.qc.ca/home.php#>