

PRIVACY POLICY

TABLE OF CONTENTS

1.0	Privacy Charter.....	1
2.0	Roles and Responsibilities	2
2.1.	Privacy Officer Responsibilities	2
2.2.	Managers.....	2
2.3.	All Staff	2
2.4.	Contractors	3
3.0	Collection of Personal information	3
3.1.	Collection and Consent Standards.....	3
3.2.	Consent Process	4
4.0	Personal Employee Information	5
4.1.	Collection for Employee Management Purposes	5
4.2.	Use and Disclosure of Personal Employee Information	5
4.3.	Employment Verification and References	5
4.4.	Employee Notification	6
5.0	Personal Information	6
5.1.	Collection for Operational Purposes.....	6
5.2.	Use and Disclosure of Personal Information	6
5.3.	Notification Requirements	7
6.0	Individuals' Right of Access and Correction.....	7
6.1.	Individual Requests for Access to Their Own Information.....	7
6.2.	Exceptions to Right of Access	8
6.3.	Individual Requests to Correct or Amend Personal Information	9
6.4.	Individual Challenges to Request Responses.....	9
7.0	Information Security and Retention.....	9
7.1.	Administrative Safeguards.....	9
7.2.	Physical Safeguards.....	10
7.3.	Technical Safeguards.....	11
8.0	Contractor Security.....	12
8.1.	Contract Provisions.....	12
8.2.	Enforcement	13
9.0	Appendices.....	14
	Appendix 1: Sample Confidentiality Agreements	14
	Appendix 2: Sample Consent Forms.....	16
	Appendix 3: Business Purposes for Personal Information	17
	Appendix 4: Sample Privacy Notification.....	20
	Appendix 5:.....	21
	Security of Facsimile and Electronic Mail Transmissions and Recordation of Telephone Conversations	21
	Appendix 6: Records Management	23
10.0	Schedules	26
11.0	Glossary of terms.....	27

1.0 PRIVACY CHARTER

Provident is committed to protecting the privacy of individual clients, employees, and associates and to meeting the highest legislative and industry standards of client companies. To that end, Provident has implemented a privacy program to meet the following privacy goals:

1. Accountability

Provident is responsible for protecting the confidentiality of personal information in its custody or under its control in compliance with the applicable federal or provincial legislation. Provident has identified and designated a Privacy Officer to be responsible for implementing the privacy program and ensuring compliance with legislation.

2. Openness

Provident develops and follows privacy and security policies and practices that are compliant with legislation and industry best practices. Such policies and practices are publicly available.

3. Collection and Consent

Provident collects personal information only for reasonable business purposes and with the consent of the individual or, without consent, in accordance with purposes authorized by legislation.

4. Identifying Purposes

Provident identifies the purposes for which personal information is collected.

5. Limited Use, Disclosure and Retention

Provident uses, discloses and retains personal information for purposes consistent with the purpose for which it was collected. Use and disclosure for other purposes is by consent of the individual or as authorized by legislation.

6. Accuracy

Provident makes all reasonable efforts to ensure that personal information collected, used or disclosed by or on behalf of Provident is accurate and complete.

7. Safeguards

Provident protects personal information in its custody or control by deploying security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

8. Right of Access

Individuals have a right to access information about themselves at Provident, subject only to limited and specific exceptions. Individuals who believe there is an error or omission in their personal information have a right to request correction or amendment of the information.

9. Compliance Challenges

Individuals are encouraged to bring any concerns or issues regarding privacy at Provident to the Privacy Officer for discussion and response. Individuals may appeal to the Privacy Commissioner of Canada or the appropriate provincial Privacy Commissioner to review or investigate Provident right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

2.0 ROLES AND RESPONSIBILITIES

Charter Principles

Accountability

Provident is responsible for protecting the confidentiality of personal information in its custody or under its control in compliance with the applicable federal or provincial legislation. Provident has identified and designated a Privacy Officer to be responsible for implementing the privacy program and ensuring compliance with legislation.

Compliance Challenges

Individuals are encouraged to bring any concerns or issues regarding privacy at Provident to the Privacy Officer for discussion and response. Individuals may appeal to the Information and Privacy Commissioner of Alberta to review or investigate Provident right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

Policy

2.1. Privacy Officer Responsibilities

The Privacy Officer is responsible for overall management and coordination of information access, privacy and security. The responsibilities and authority of the Privacy Officer include:

- identifying privacy compliance issues for Provident;
- ensuring that privacy and security policies and procedures are developed and maintained as necessary;
- ensuring that Provident staff and contracted personnel are aware of their duties, roles, and responsibilities under applicable privacy legislation;
- providing advice on, and interpretation of, applicable privacy legislation, including release / non-release of information;
- responding to requests for access to information, or to correct or amend personal information, and facilitating the request process as necessary;
- gaining access to company information required to respond to requests and inquiries, investigate incidents, and administer security;
- ensuring the overall security and protection of personal information in the custody or control of Provident;
- representing Provident in dealings with third parties, the provincial or federal government, and the privacy regulator, as necessary.

2.2. Managers

Provident Management reviews and approves Privacy policy.

2.3. All Staff

All staff are responsible for implementing privacy for all information they may collect, use, disclose, handle, or view. Staff members:

- make themselves aware of and adhere to access to information and privacy policies and standards;
- access, release and protect information in their custody or control according to policy;
- refer to the Privacy Officer all decisions about collection, use, disclosure, and access that are not clearly directed by policy.

2.4. Contractors

Provident is responsible for all personal information generated by external services providers completing contracted services for Provident. For external service providers which have exposure to and use Provident information assets and systems, Provident requires contracted third parties to:

- Report breaches of confidentiality and privacy to Provident's Privacy Officer.
- Sign an agreement with Provident detailing explicit information security and privacy provisions when given access to premises or systems containing confidential business or personal information of Provident.
- Make information security and privacy policies available to Provident upon request, including any updates or revisions that occur after execution of the contract.
- sign a confidentiality (non-disclosure) agreement (see [Appendix 1](#))
- include provisions in a contract that protect Provident operations from circumstances where the information assets or systems may be compromised, including disaster recovery and system backup that meets or exceeds that of Provident.

Provident retains the right to inspect contractor premises and security practices to ensure compliance with contract provisions and stated policies.

3.0 COLLECTION OF PERSONAL INFORMATION

Charter Principles

Collection and Consent

Provident collects personal information only for reasonable business purposes and with the consent of the individual or, without consent, in accordance with purposes authorized by legislation.

Identifying Purposes

Provident identifies the purposes for which personal information is collected.

Limited Use, Disclosure and Retention

Provident uses, discloses and retains personal information for purposes consistent with the purpose for which it was collected. Use and disclosure for other purposes is by consent of the individual or as authorized by legislation.

Policy

3.1. Collection and Consent Standards

1. Provident obtains the consent of the individual before collecting the information. If additional consent is required for use and disclosure consent will be obtained from the individual before the use or disclosure occurs.
2. There are three options for determining the appropriate consent forms or process:
 - *Explicit consent:*
Individual is properly informed and explicitly gives permission, either in writing or orally, before action taken. See [Appendix 2](#) for sample consent form.
 - *Implied or deemed consent:*
Permission is reasonably implied based on clear and direct actions and circumstances under which the information was provided, without even notifying the individual of the purposes.

- *Opt-out:*
An individual is given reasonable opportunity to express their wishes; if no response is given, consent is assumed.
3. Explicit or implied consent is required for collection of all personal information, unless specifically authorized in policy.
 4. Opt-out is only used when dealing with personal information limited to name and location or contact information.
 5. Only the individual or authorized representative can provide consent.
 6. Provident cannot refuse a service to an individual if they refuse to give their consent for the collection of personal information beyond what is reasonably required to provide the service.
 7. An individual may refuse to give their consent for personal information to be collected in relation to a specific purpose Provident has identified. In the event that an individual places reasonable conditions on their consent, Provident must consider whether there is another way the purpose may be achieved without collecting the information.
 8. An individual may revoke consent at any time.
 9. Personal information that is not health information is deemed to have been collected with appropriate consent and notification if it was collected before January 1, 2004.

3.2. Consent Process

1. Where personal information is collected before the written consent can be signed, the Provident staff member will explain the elements of the consent and note verbal consent in the appropriate documentation.
2. Only the individual or authorized representative can provide consent.
3. Provident cannot refuse a service to an individual if they refuse to give their consent for the collection of personal information beyond what is reasonably required to provide the service.
4. An individual may refuse to give their consent for personal information to be collected in relation to a specific purpose Provident has identified. In the event that an individual places reasonable conditions on their consent, Provident must consider whether there is another way the purpose may be achieved without collecting the information.
5. An individual may revoke consent at any time by notifying Provident. Notification may be in writing or by another form of communication.

4.0 PERSONAL EMPLOYEE INFORMATION

4.1. Collection for Employee Management Purposes

Personal employee information collected must be limited to that required to support the work or relationship the employee has with Provident. The purposes for collection of personal employee information may include:

- Enabling professional development
- Ensuring employee health and safety
- Processing salary payments
- Obtaining contract services
- Human resources administration
- Evaluation of staff / performance appraisals
- Employee recruitment, classification and compensation
- Employee evaluation
- Occupational health and employee benefits administration
- Verification of employment or education (reference checks)

The purposes for collection of personal employee information, including the specific function and activities listed in [Appendix 3](#).

4.2. Use and Disclosure of Personal Employee Information

Consent is not required for the use and disclosure of Personal Employee Information in the following circumstances:

- it is clearly in the best interests of the individual and consent cannot be obtained in a time period required for the purpose;
- to conduct an investigation of a breach of law or agreement or for a legal proceeding;
- to deal with an emergency that threatens the life, health or security of an individual;
- to comply with a subpoena or warrant;
- to collect a debt owed by the individual to Provident;
- for archival or research purposes that cannot be achieved without using identifiable information;
- if the collection is authorized by statute or regulation;
- to support legal counsel in order to represent Provident;
- to contact next of kin or friend of an individual who is deceased, ill, or injured;
- to determine the individual's suitability to receive an honor, award or similar benefit, including an honorary degree, scholarship or bursary.

Consent is not required when personal information is collected for the purposes of recruiting potential employees, managing an existing employee, or terminating an employee. For all other purposes, Provident will obtain the consent of the individual using the Consent Form (see [Appendix 2](#)) to authorize the collection of personal employee information and in accordance with consent standards.

4.3. Employment Verification and References

Under Alberta's *Personal Information Protection Act*, Provident may conduct employment verification or reference checks for potential employees without their consent. Similarly, Provident may provide employment reference checks without the consent of the individual.

Under the federal PIPEDA, consent must be obtained from the former employee if more than the employee's date of hire and termination and position is disclosed. Employment references may only be provided where the individual being requested to provide a reference is a named reference (see [Appendix 2](#)) and consent has been provided by the individual before the reference check is conducted.

4.4. Employee Notification

Whether or not consent is required, all potential, existing, and past employees will be notified of the purposes for which their personal employee information is collected, used, and disclosed before the information transaction takes place.

1. Provident notifies individuals through the use of appropriate forms, letters, verbal statements, brochures, or other forms of communication [Appendix 4](#) on all application forms.
2. Other employment management purposes: Provident includes the notification statement in [Appendix 4](#) on all letters of employment.

5.0 PERSONAL INFORMATION

5.1. Collection for Operational Purposes

Provident collects the least amount of information with the highest degree of anonymity, to meet only a reasonable business purpose. For further details about the purposes for the collection, use or disclosure of personal information, please refer to [Appendix 3](#).

Provident collects personal information about individuals directly from the individual the information is about or authorized representative.

Health information and other personal information can be collected without the consent of the individual for the following purposes:

- it is clearly in the best interests of the individual and consent cannot be obtained in a time period required for the purpose;
- to conduct an investigation of a breach of law or agreement or for a legal proceeding;
- to deal with an emergency that threatens the life, health or security of an individual;
- to comply with a subpoena or warrant;
- to collect a debt owed by the individual to Provident;
- for archival or research purposes that cannot be achieved without using identifiable information;

Personal information *other than health information* can be collected without the consent of the individual for the following additional purposes:

- if the collection is authorized by statute or regulation;
- to support legal counsel in order to represent Provident;
- to contact next of kin or friend of an individual who is deceased, ill, or injured;
- to determine the individual's suitability to receive an honor, award or similar benefit, including an honorary degree, scholarship or bursary.

5.2. Use and Disclosure of Personal Information

Provident uses and discloses personal information only for the purposes consistent with those identified at the time of collection or according to purposes listed in [Appendix 3](#). All uses and disclosures for other purposes requires the consent of the individual.

Consent is not required for the disclosure of both health and personal information, regardless of the purposes for which it was collected, in the following circumstances:

- to government agencies, or investigative bodies with the authority to administer or enforce a law of Canada, or to investigate a threat to national defense, security, or international affairs;
- to comply with a statute or regulation.

In addition, personal information other than health information can be disclosed without the consent of the individual to a surviving spouse, partner or relative of a deceased individual if the disclosure is reasonable.

5.3. Notification Requirements

Provident ensures that the individual is properly notified of the purposes for collecting, using or disclosing their personal information before the information transaction takes place, unless it is for one of the purposes for which consent is not required.

Provident ensures individuals are notified of any surveillance devices in use on the premises for security purposes.

Provident notifies individuals through the use of appropriate notices, forms, posters, verbal statements, brochures, or other forms of communication. See [Appendix 4](#) for sample notification.

6.0 INDIVIDUALS' RIGHT OF ACCESS AND CORRECTION

Charter Principles

Right of Access

Individuals have a right to access information about themselves at Provident, subject only to limited and specific exceptions. Individuals who believe there is an error or omission in their personal information have a right to request correction or amendment of the information.

Compliance Challenges

Individuals are encouraged to bring any concerns or issues regarding privacy at Provident to the Privacy Officer for discussion and response. Individuals may appeal to the Privacy Commissioner of Canada or the appropriate provincial Privacy Commissioner to review or investigate Provident right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

Policy

6.1. Individual Requests for Access to Their Own Information

1. Requests from individuals to access basic personal information about themselves (e.g., contact information, dates and times) are handled as a routine release of information.
2. Formal requests for access to information that may involve review and severing must be in writing to Provident's Privacy Officer, or designate. An individual may request access to another person's information only if they have signed consent of the person or if they can prove they are the person's legal representatives.
3. Individuals making routine or formal requests may be required to provide sufficient information to verify their identity and authorize access to the information. Any such information provided shall be used for these purposes only.
4. Provident responds to formal requests for access to personal information within forty-five (45) calendar days of receipt of the request and within thirty (30) calendar days for requests for health information.
5. Provident does not charge the individuals for access to their own personal information. However, reasonable fees may be charged for reproduction, transcription, or transmission of information, so long as the individual is notified before these costs are incurred. A fee for reasonable costs incurred may be charged when responding to more complex requests. The individual will be informed of the fee in advance.

6. Requested information will be provided in a form that is generally understandable. Provident will endeavor to explain the meaning of the content, codes and abbreviations included in the individual's record to the extent that it is reasonably practical.
7. In providing an account of third parties to whom it has disclosed personal information about an individual, Provident will be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, Provident will provide a list of organizations to which it is likely to have disclosed information.
8. Individuals are permitted to view either the original record, or to request a copy of the record, subject to exceptions under the Act. To preserve the integrity of the record and ensure that documents are not removed from Provident, an individual wishing to view an original record will do so under the supervision of designated personnel.

6.2. Exceptions to Right of Access

1. In certain situations, Provident may not be able to provide to an individual access to all the personal information it holds about them.
2. Provident must not release to the individual making the request personal information about another individual without the other individual's consent.
3. Provident may refuse to provide access to personal information:
 - if access could reasonably be expected to threaten the life or security of another individual.
 - that is protected by solicitor-client privilege;
 - that would reveal confidential commercial information;
 - that was collected without the individual's knowledge or
 - consent as part of an investigation of a breach of agreement or contravention of law;
 - that was generated in the course of a formal arbitration or
 - mediation process;
 - that is about disclosures of information to comply with a
 - warrant or subpoena.
4. In addition, for personal information other than health information, Provident
 - must refuse to provide access to information when it reveals the identity of a third party providing an opinion about an individual, unless the third party consents to the access;
 - may refuse to provide access if disclosure might result in that type of information no longer being supplied and it is reasonable for Provident to require that type of information for its business purposes.
5. Provident will always provide access if it is needed because an individual's life, health, or security is threatened.
6. In the event that Provident refuses to provide access to information, the excepted information is appropriately severed from the record before providing it to the individual.
7. Provident informs the individual in writing of the refusal or acceptance of the request, the reason(s) for the refusal, and any recourse the individual may have to challenge the decision.

6.3. Individual Requests to Correct or Amend Personal Information

1. Requests from individuals to correct / amend information about themselves (e.g. change of name or address) are handled as a routine correction of information.
2. Formal requests to correct or amend information subject to review must be in writing to Provident's Privacy Officer, or designate. An individual may request the correction of another person's information only if they have that person's signed consent or they can prove they are the person's legal representative.
3. All formal requests must be accompanied by appropriate documentation to support their request before Provident will amend the information as required and as appropriate. Generally, Provident will not amend professional opinions that are made by staff that have the competency to make them. If amendments are made, the original information must not be deleted but retained and marked as incorrect by crossing out, for example. The amended information will be transmitted to third parties, as appropriate.
4. Provident responds to formal requests for correction of personal information within forty-five (45) calendar days of receipt of the request and within thirty (30) days for requests involving health information.
5. Provident informs the individual in writing of the refusal or acceptance of the request, the reason(s) for the refusal, and any recourse the individual may have to challenge Provident's decision.
6. If the individual is not satisfied with the results of his/her request, Provident internally documents the issue in the relevant record(s) and provides a response. The existence of the unresolved challenge will be transmitted to third parties, as appropriate.

6.4. Individual Challenges to Request Responses

Individuals are encouraged to bring any concerns or issues about responses to requests or compliance with this policy to Provident's Privacy Officer for discussion and mediation. Individuals may also challenge responses in writing to the Information and Privacy Commissioner of Alberta or, in the case of health information, the Privacy Commissioner of Canada.

7.0 INFORMATION SECURITY AND RETENTION

Charter Principles

Safeguards

Provident protects personal information in its custody or control by deploying security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Policy

7.1. Administrative Safeguards

1. The need for confidentiality and security of information is addressed as part of the conditions of employment for Provident staff, beginning with the recruitment stage, and included as part of job descriptions and contracts (see sample [Confidentiality Agreement](#)). The performance of individuals is monitored to reduce the risk of error, fraud, or misuse of information. All staff are made aware of, and appropriately trained in, policies and procedures for safeguarding information.
2. All Provident staff, volunteers, and contracted personnel that collect, use, disclose or have access to confidential information as part of the performance of their duties for Provident.

3. Provident only uses and discloses the least amount of information necessary for the intended purpose, and only to staff with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information is made anonymous.
4. Before implementing proposed new administrative practices or information systems that change or affect significantly the collection, use and disclosure of health information, Provident completes an assessment that describes how the new initiative will affect privacy, and what measures Provident will put in place to mitigate risks to privacy.
5. Provident staff report all violations and breaches of information security as soon as possible to Provident Privacy Officer in order that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence. The nature of the response is determined according to the level of gravity of the breach or violation.

7.2. Physical Safeguards

1. All Provident records, both on-site and off-site, are held and stored in an organized, safe and secure manner in accordance with information security standards.
2. Provident records are not left in on-site or off-site areas accessible by unauthorized persons unless the area is under supervision. At reception desks or offices where unauthorized persons are present, no files is left unattended or accessible;
3. Computers or monitors that are left unattended in reception areas or areas where personal information is processed are secured and logged off, either manually or by default timer.
4. All servers and equipment storing electronic personal information are secured by locked cabinets or rooms within Provident when not under direct supervision by Provident staff.
5. Provident records or equipment holding personal information (e.g. laptop computers) should not be left unattended in a vehicle, even if the vehicle is locked.
6. Appropriate measures are taken to control the distribution of keys or pass codes, and to ensure they are returned or changed after their employment by Provident has ended.
7. A staff member accompanies visitors to Provident areas where personal information is processed.
8. Confidential information is not be transmitted verbally if conversations can be overheard or intercepted.
9. Confidential, restricted, or sensitive information that is transmitted by mail or courier is be sealed, marked as confidential, and directed to the attention of the authorized recipient.
10. Provident staff must verify the identity and credentials of courier services used for the transportation of personal health information. Provident supervises couriers or shippers accessing mailrooms where personal information is stored or processed.
11. Fax machines and printers that may be used to send or receive personal information are located in a secure area. Whenever possible, staff use preprogrammed numbers to send fax transmissions, and must review the numbers every 6 months to ensure they are still accurate. All fax transmissions should be sent with a cover sheet that indicates the information being sent is confidential (see [Appendix 5](#)). Reasonable steps are taken to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine.

12. Personal information is retained on for as long as reasonably required for business purposes, and in accordance with Provident's Record Retention Schedule. Transitory records such as copies of document, meeting dates, etc., are destroyed as quickly as possible (see [Appendix 6](#)).
13. Information that is not confidential or sensitive in nature should be disposed of by placing it in recycling bins. Confidential or sensitive information is disposed of by shredding. Destruction of personal information, other than transitory records, is documented by listing the records / files to be destroyed, recording the date of destruction, and having a staff member sign off that the destruction occurred.
14. All information is deleted using secure data wiping techniques prior to disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) are destroyed.
15. Information that is intended for long-term storage on electronic media (e.g. tape, DVD, disk) are reviewed on an annual basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

7.3. Technical Safeguards

1. Provident deploys firewalls, intrusion detection software, or other technical means to protect internal Provident networks carrying identifiable personal information from unauthorized use and malicious software.
2. All Provident information systems users are assigned a unique identifier (User ID) that restricts access to data and application systems to that information based on their functional roles and need to know.
3. Provident staff only access and use information systems under their assigned User ID. The use of another person's assigned User ID is prohibited.
4. Access to Provident information systems is controlled and password protected. Passwords are kept confidential at all times and are not written down, posted publicly, or shared with other staff. Passwords will be changed every 45 days. If a computer is left unattended, it is protected against unauthorized access by either manual or automated logout requiring authentication to re-enter the system.
5. Confidential personal information is not be sent by e-mail or transmitted over the internet or external networks without the use of appropriate security measures such as encryption and authentication. E-mail messages containing personal information include a confidentiality notification (see [Appendix 5](#)).
6. To detect unauthorized access and prevent modification or misuse of user data in applications, systems are monitored to ensure conformity to access policies and standards. Appropriate security controls, such as event logs, are implemented and reviewed as required.
7. Computer systems that hold critical or sensitive information are backed up on a daily basis. Steps are taken to ensure that backed up information is stored in a secure environment off-site.

8.0 CONTRACTOR SECURITY

Charter Principles

Accountability

Provident is responsible for protecting the confidentiality of personal information in its custody or under its control in compliance with the applicable federal or provincial legislation.

Safeguards

Provident protects personal information in its custody or control by deploying security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Policy

8.1. Contract Provisions

1. Provident is responsible for all personal information generated by external services providers completing contracted services for Provident.
2. All external service providers that require access to the information systems and assets of Provident complete and sign an agreement with Provident detailing explicit information security and privacy provisions.
3. Until such a contract has been executed, no personal information is disclosed to the external service provider and the external service provider is not given access to premises or systems containing confidential business or personal information of Provident.
4. Information security provisions outlined in contracts with external service providers meet or exceed the standards set out in Provident information security policies and procedures. Any related external service provider information security and privacy policies are made available to Provident upon request, including any updates or revisions that occur after execution of the contract.
5. All employees and contractors who have exposure to and use Provident information assets and systems shall sign a [confidentiality \(non-disclosure\) agreement](#). External service providers remind their employees on termination of their continued responsibility to maintain the confidentiality of Provident information.
6. Provident requires contracted third parties to report breaches of confidentiality and privacy to Provident Information Privacy Officer.
7. Contracts with external service providers that have access to Provident information assets and systems include provisions that protect Provident operations from circumstances where the information assets or systems may be compromised. In order to mitigate these situations, disaster recovery and system backup must be included in all agreements, to a standard that meets or exceeds that of Provident.
8. Contracts with external service providers include provisions for destroying or returning all Provident information assets, including hardware, system documentation and information assets upon termination of agreements and in accordance with contract provisions reflecting records retention and data management policy.

8.2. Enforcement

1. To ensure compliance with contracted provisions for information security, Provident:
 - requests contractors sign an acknowledgement that they have received, read and will comply with any Provident information security policies they are bound to follow under contract;
 - actively monitors external service providers with access to information assets or systems for inappropriate access or use and to ensure compliance with contract security provisions.
2. Provident retains the right to inspect contractor premises and security practices to ensure compliance with contract provisions and stated policies.

9.0 APPENDICES

Appendix 1: Sample Confidentiality Agreements

[Note: to be attached with Offer Letter]

Employee Confidentiality Agreement

I, _____ agree that, as an employee / volunteer / contracted service provider of Provident, I will observe and comply with all policies and procedures of Provident with respect to privacy, confidentiality, and security of personal information, including personal health information.

Unless legally authorized to do so, I will not access or disclose personal information, including personal health information that comes to my knowledge or possession by reason of my affiliation with Provident.

I understand that a breach of this agreement may be just cause for termination of my employment or affiliation with Provident.

I am aware that Provident has policies and procedures regarding the privacy, confidentiality, and security of personal information and personal health information and I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures.

I understand that I can refer to Provident's Privacy Officer for the details of these policies.

Signature

Printed Name

Date

Contractor Confidentiality Agreement

I, _____ agree that, as an employee / volunteer / sub-contractor of [*contracted company*] providing services to Provident, I will observe and comply with all policies and procedures of Provident with respect to privacy, confidentiality, and security of personal information, including personal health information of the Company.

Unless legally authorized to do so, I will not access or disclose personal information, including personal health information that comes to my knowledge or possession by reason of my work or affiliation with Provident.

I understand that a breach of this agreement may be just cause for termination of my employment with [*contracted company*] and affiliation with Provident.

I am aware that Provident has policies and procedures regarding the privacy, confidentiality, and security of personal information and personal health information and I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures.

I understand that I can refer to the Provident's Privacy Officer for the details of these policies.

Signature

Printed Name

Date

Appendix 2: Sample Consent Forms

Personal Information Consent Form

I, _____, consent to Provident collecting, using or disclosing personal information for reasonable business purposes, specifically:

< See [Appendix 3](#) for list of business purposes and personal information > Example:

Payment of Royalties:

For the purpose of receiving Royalty Payment from Provident Energy Ltd, this information may include my name, address, telephone number, social insurance number, residency and tax information.

I understand that Provident is subject to provincial and federal privacy legislation and has in place a Policy on Privacy to ensure compliance with privacy legislation and standards.

I am aware of the risks and benefits associated with consenting or not consenting to collection, use or disclosure and that I may revoke my consent at any time by providing a signed, written statement of revocation to Provident.

Signature: _____

Date: _____

Reference Check Consent Form

(Note: Under PIPA, Provident does not require the consent of the individual to collect employment references)

I, _____, authorize Provident to contact the individuals listed below for the purpose of obtaining employment reference information about me.

Organization Name

Contact Name, Title

Telephone Number

I understand that Provident is subject to provincial and federal privacy legislation and has in place a Policy on Privacy to ensure compliance with privacy legislation and standards.

I am aware of the risks and benefits associated with consenting or not consenting to collection, use or disclosure and that I may revoke my consent at any time by providing a signed, written statement of revocation to Provident.

Printed Name _____

Date: _____

Signature: _____

Appendix 3: Business Purposes for Personal Information

Personal Employee Information

The following personal information may be collected in relation to specific business purposes. These purposes may be identified and applied as necessary to consent for collection, use, or disclosure and to notification documents.

<i>Business Purpose</i>	<i>Personal Employee Information</i>
<i>Staffing and Employee Management</i>	
Recruitment Contracting Personnel Management	<ul style="list-style-type: none"> • resume (phone/address education info etc). • grievance information • Code of conduct • References • performance reviews • records of training performance/evaluations • Emergency contact information • Offer letter
Compensation	<ul style="list-style-type: none"> • Salary / Wage Information • Training Certificates • Awards and Recognitions • Employee performance evaluations • Employee investigations • letters of salary adjustments
Payroll	<ul style="list-style-type: none"> • Personal Banking information (account number, SIN) • General payroll Information (CPP, EI, Benefit deductions) • Attendance Schedules (Holiday, Leave of Absence) • TDI • Garnishees
<i>Benefits</i>	
Insurance Pension	<ul style="list-style-type: none"> • Name • Social Insurance Number (SIN) • Salary • Family or individual coverage • Alberta Health Care Number • Beneficiaries • Policy / benefit preferences
<i>Employee Health and Safety</i>	
Physical security of Provident properties and premises	Names information for people that would require assistance in emergency situations <ul style="list-style-type: none"> • Home phone number

<i>Business Purpose</i>	<i>Personal Employee Information</i>
Injury Reporting Workers Compensation	<ul style="list-style-type: none"> • Medical assessment information • Name • Age • Description of incident • Environmental/exposure assessments • WCB reporting form(s)
Risk Mitigation and Security Law Compliance	Voices of those employed as traders Content of telephone conversations made during the course of trade activity
<i>Corporate Operation</i>	
Board of Directors	Birth date Social Insurance Number (SIN) Consent form <ul style="list-style-type: none"> • Name, phone number

Personal Information for Operational Purposes

The following personal information may be collected in relation to a specific operational purpose.

These purposes may be identified and applied as necessary to consent for collection, use, or disclosure and to notification documents.

Operational Purpose/Activity	Personal Information
Environmental Health and Safety	
Emergency Response Planning	Resident listing: <ul style="list-style-type: none"> • includes names, ages of children and adults • school (pick-up and drop-off times), • environmental sensitivity e.g. asthma • Physical evacuation assistance requirements • telephone, address, e-mail address, house style and exterior
Investor Relations	
Communication with shareholders	<ul style="list-style-type: none"> • Name, address, phone number and e-mail to maintain the mailing list
Royalty Payables	<ul style="list-style-type: none"> • T5 / NR4's Names and address of royalty owners (Crown Royalty, Freehold Royalty) • Human Resource Records • Name • Social Insurance Number • Tax Information • Home address • Home telephone number • Non-Resident Information
Land and Contracts	
Surface, Unit, facilities easements	<ul style="list-style-type: none"> • Landowner personal contact information • Royalty Rates • Compensation Information (amount paid to get lease) • Estate information • Social Security Numbers (SSN) for freehold individuals in the US (to pay rentals) • Non-resident information
Business Contracts	<ul style="list-style-type: none"> • land purchase / trade information • Resumes: Legal contracts, bids, service agreements • telephone numbers for business contact purposes
Risk Mitigation	
Security Law Compliance	Voices of those employed as traders Content of telephone conversations made during the course of trade activity

Appendix 4: Sample Privacy Notification

Notification statement for Application Forms

Provident collects this information solely for the purposes of assessing your suitability as a candidate for employment. Reference check information will be collected for individuals who have advanced to the final stages of the recruitment process. No disclosure of information contained on a resume or other personal information, such as reference information, will occur without your permission, unless required or authorized by law.

You may withdraw your consent at any time by providing a signed, written statement of revocation to Provident Energy.

The information of unsuccessful applicants will be retained for a maximum of one year after the close of the competition. Provident is subject to provincial and federal privacy legislation. If you have questions about Provident's privacy practices, you may contact the Privacy Officer at _____.

Notice included in Letters of Hire

Provident collects uses and discloses personal information for the following employment management purposes, and risk mitigation purposes only, unless required or authorized by law:

- *Employee Management* including payroll, recruitment, compensation, and supervision: employee contact information, salaries, accounts, employment histories, references, evaluations, investigations, and employment record
- *Employee Benefits* including insurance application and benefits updates
- *Staff Communication* including emergency contact information
- *Risk Mitigation and Security Law Compliance - telephone conversations conducted by traders in the course of trade activity*

Provident is subject to provincial and federal privacy legislation. For questions about Provident's privacy practices, please contact the Privacy Officer at _____

Appendix 5:

Security of Facsimile and Electronic Mail Transmissions and Recordation of Telephone Conversations

All Transmissions

1. Limit transmission to circumstances where it is immediately necessary for time-sensitive or functional reasons and to the least amount of information possible.
2. All transmissions must be accompanied by the following statement:

This information is intended for the identified recipient only and may contain information that is privileged or confidential under law. If you are not the intended recipient, you are hereby notified that any dissemination or communication of this information is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the contact address or number indicated.
3. Provident users will only send or forward very large documents or attachments when absolutely necessary.
4. Provident will protect of data awaiting output to a level consistent with its sensitivity. Only those authorized should see the data.

Electronic mail

1. Do not transmit by e-mail over a service other than the regional e-mail service (e.g., hotmail)
2. Remove all personal identifiers from the message if possible.
3. Do not transmit identifiable personal information by e-mail to an external or public zone unless the information is secured by encryption.
4. Do not include identifiers or personal information in the subject header of the mail.
5. Verify all addresses as correct before sending messages.
6. Develop, update and use e-mail addresses from address book.
7. Request notification of receipt.
8. Provident users will not open e-mail message Attachments from suspicious or doubtful sources. If in doubt, contact the sender and verify the content of the message.
9. Include a confidentiality / privacy statement in all outgoing e-mail messages, for example:

This email communication is intended as a private communication for the sole use of the primary addressee and those individuals listed for copies in the original message. The information contained in this e-mail is private and confidential and if you are not an intended recipient you are hereby notified that copying, forwarding or other dissemination or distribution of this communication by any means is prohibited. If you are not specifically authorized to receive this e-mail and if you believe that you received it in error please notify the original sender immediately. We honor similar requests relating to the privacy of e-mail communications.

Fax Transmissions

1. The recipient's machine must be in a secure area. Otherwise, the recipient should stand by to receive and confirm transmission of the information. Where information is routinely sent by batched fax transmission, the responsibility to confirm secure receipt of the information lies with the sender.

2. An approved Provident Fax Transmission Cover Sheet must be completed and accompany the information transmitted.
3. To ensure accuracy in dialing, confirm the number being dialed by visual check on the fax machine display. For frequently dialed numbers, use the automatic dialing feature to minimize incorrect dialing.
4. For automatic faxing by computer, use a fax table for automatic dialing of numbers.
5. Where possible, use available security features on the fax machine, i.e. confidential mailboxes to ensure the confidentiality of information.
6. Print out and check the fax machine logs after transmission to verify that documents were received at the correct number.
7. If it is determined that the transmission was received by a wrong number:
8. contact the recipient and ask them to return or destroy the documents,
9. retain copies of all information sent, and,
10. report the incident as an information security breach to Provident's Privacy Officer.

Inspections of E-mail Messages

1. Provident may view, monitor or inspect any messages sent or received using Provident system in order to:
 - investigate information security incidents
 - support an urgent, time-sensitive action
 - maintain Provident information systems
 - comply with a court order or statutory requirement
2. Where access to e-mail is deemed necessary, Provident will attempt to inform the affected users prior to any inspection disclosure of e-mail records, except when such notification would be detrimental to an investigation of possible violation of the Act or Provident policy.

Filing and Retention of E-mail messages

E-mail messages are considered records and therefore subject to Provident retention policies. Messages that must be retained as master records should be either:

- printed out and filed in the appropriate paper file
- transferred from the e-mail directory to a secure and maintained electronic file director

Recordation of Telephone Conversations

Telephone conversations between traders employed by Provident and outside traders may be recorded for the purposes of compliance with security legislation and for risk mitigation purposes. Only telephone conversations made during the course of trade activity will be recorded.

Appendix 6: Records Management

The Records Retention Schedule defines administrative and operational record series, assigns accountability for the original records in each series to a department, and instructs users on when to move records from active office space to semi-active storage and/or provide for their destruction. The Records Retention Schedule includes a standardized classification scheme providing a common means for effective storage, retrieve and cross reference of records

1. Records Registration Process

Provident will keep a records registry of all non-transitory records whether paper or electronic. The records registry is an inventory of all Provident records series. A record series is a grouping of individual files or records maintained together because of common function, system, subject, and/or format.

Provident staff, affiliates, and contractors will record all non-transitory records series in their custody or departmental area, whether paper or electronic.

2. Transitory Records

Provident Records Classification and Retention Schedule does not apply to transitory records. Transitory records are drafts, copies, or short-term information. Transitory records:

- must be kept to a minimum;
- must be securely stored and destroyed

Staff are responsible for identifying transitory information in their custody and destroying it after it is no longer needed. The following criteria may be used in determining which records are transitory:

Transitory Record Type	Description
<i>Temporary Purpose</i>	The records have a very temporary, insignificant or routine purpose (e.g., phone messages, routing slips, Post-It notes, meeting schedules, diaries, routine requests, invitations, notices of meetings, cover sheets)
<i>Copies of Master Records</i>	The records are direct copies of files or groups of master records kept elsewhere by the office of record (e.g., copies of minutes, reports, data files).
<i>External Publications</i>	The records are external publications that are no longer required for operations (e.g., books, articles, newspapers, brochures, manuals).
<i>Unsolicited Material</i>	The records were received as unsolicited direct mail (e.g., advertisements, unsolicited resumes).
<i>Blank Forms and Templates</i>	The records are blank information media (e.g., blank obsolete forms, disks, videos or tapes).

Transitory Record Type	Description
Working Papers, Background Data, Drafts	<p>The records are draft notes that were used in the preparation of documents and are no longer required (e.g., drafts of reports, working notes or tapes, some raw data).</p> <p>NOTE: draft records that contain information relating to accountability and/or historical relevance should be retained. Caution should be taken before destroying drafts produced in completion of the following types of documents:</p> <ul style="list-style-type: none"> • legal agreements • audit reports • policies, standards, and guidelines • medical or scientific records • corporate publications and communications materials

3. Records Security Classification

Provident staff and contractors will use the *Information Security Classification and Standards Table* to determine an appropriate security classification for each record series, file or document in their custody. The departmental supervisor is accountable to ensure all record series in the custody of their department are handled appropriately for their security classification.

Provident staff and contractors will assign and document the security classification to each series, file or document as part of the Records Registration Process.

Information Security Classification and Standards Table					
Class	Harm	Information Type	Security Zones	Copying	Destruction
Restricted R	<ul style="list-style-type: none"> • Harm to operations of facilities or security systems of Provident • Immediate harm to health and safety of residents, clients, or staff • Loss of source record and accountability 	<ul style="list-style-type: none"> • Information describing Provident security systems, access codes, etc. • Personal information that would likely cause or allow a person to harm themselves or other persons • Back-up or archival copies of essential records and confidential records 	Network: Restricted Physical: Restricted	No copying	Supervised on-site shredding or data wiping and destruction logged

Information Security Classification and Standards Table					
Class	Harm	Information Type	Security Zones	Copying	Destruction
Confidential C	<ul style="list-style-type: none"> • Harm to health and safety of residents, clients, or staff • Economic loss for Provident or third parties • Damage to credibility or service integrity of Provident • Legislative sanctions • Loss of source record and accountability 	<ul style="list-style-type: none"> • All personal health information • Employee and health provider information • Information given in confidence or under privilege • Quality assurance records • Third party business information • Deliberations, investigations, advice, decisions • Security audit tools 	Network: Internal preferred; External by approval Physical: Internal preferred; External by approval	Only for backup or when access to original impractical; destroy immediately after use	Confidential shredding or data wiping (on or offsite) and destruction logged
Internal Use I	Loss of source record and accountability	<ul style="list-style-type: none"> • Staff circulars • Administrative records available to public upon request, e.g., completed decisions, policies, reports • Source records of public information 	Network: Internal or External Physical: Internal or External; Restricted for archival	No restrictions	Destruction logged
Public P	No identified harm	<ul style="list-style-type: none"> • Published materials such as pamphlets, newsletter, annual reports • Public information such as directories or web sites 	No restrictions	No restrictions	No restrictions

Provident staff and contractors will identify and mark R-level records in their custody:

Paper records

Mark each record by clearly writing or fixing the letter “R” on the top right hand of each page. Groups of R-level documents are marked on the file folder cover and back.

Electronic records

Attach the appropriate symbol on the most solid and visible surface of the storage media such as disks or videotapes, making sure not to damage the document. Electronically flag or mark the directories, files or records that store the information.

10.0 SCHEDULES

- Schedule 1: Privacy Officer and Designate(s)

Privacy Officer

Name, Title	Term
Lynn M. Rannelli, Assistant Corporate Secretary	Ongoing

Designate (s)

Name, Title	Term
Mark. N. Walker, Senior VP Finance & CFO	Ongoing

11.0 GLOSSARY OF TERMS

Applicant:

An individual who has made a formal request for access to personal information or a request for correction under PIPEDA or PIPA.

Collection:

to gather, acquire or obtain personal information from any source, including third parties.

Commercial Activity:

Any particular transaction, act or conduct, or any regular course of conduct that is of a commercial character.

Consent:

A voluntary agreement that allows the collection, use and disclosure of personal information by Provident for a defined purpose. Consent may be explicit, implied or opt-out and may be revoked at any time.

Control of Records:

A record is under the control of Provident when the organization has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Custody of Records:

Provident has custody of a record when the record is in the possession of the organization.

Disclosure:

Making personal information available to an external individual or organization, including a contractor.

Employee:

An individual employed by Provident. Under the *Personal Information Protection Act*, an individual who is an apprentice, volunteer, participant, student or who is under a contract or agency relationship is also considered an “employee.”

Explicit consent:

Individual is properly informed and explicitly gives permission, either in writing or verbally, before collection, use or disclosure of their personal information takes place. The consent form included as [Appendix 1](#) includes the elements required to ensure that explicit consent is informed and complete.

Health Information:

Personal information that is about the physical or mental health of someone, including information regarding current medication, injuries, and fitness, and the information is *not* collected for employee management purposes, either about Provident employees or the employees of a client company (e.g., occupational health, fitness to work information)

Implied Consent:

Permission is implied based on actions and circumstances of the individual where the requirement to collect, use or disclose the information is clearly related and necessary to the service provided.

Legal Proceedings:

Activities governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal

Legal Representative:

Any person who can exercise the rights or powers of an individual. This includes the right of access to an individual's personal information and the power to provide consent for disclosure of such information.

This may include:

- A guardian of a minor
- A guardian or trustee appointed under legislation, in accordance with the guardianship or trustee order
- A deceased individual's personal representative if the exercise of the right or power relates to the administration of the estate;
- An agent designated by personal directive if the directive so authorizes;
- A person who has power of attorney granted by the individual if the exercise of the right or power relates to the powers or duties conferred by the power of attorney;
- Any person with written authorization from the individual to act on the individual's behalf.

Note that family members are not legal representatives unless they have legal authority by guardianship, legislation, directive, or order.

Notification:

An explanation of policies, procedures, consequences and risks related to the collection, use or disclosure of an individual's personal or personal employee information. Provident must properly inform and notify individuals and employees when personal information is being collected, and the purposes for which it is being collected.

Opt-out Consent:

Individual is given reasonable opportunity to exercise consent; if no response is given, consent is assumed

Personal Employee Information:

Personal information collected, used, or disclosed solely for the purposes of establishing, managing or terminating an employment or volunteer relationship.

Personal Information:

Information about an identifiable individual, including factual information and opinions expressed about and by the individual, including, but not limited to:

- Name, address, age, gender, weight and height
- Educational or financial history
- ID numbers, place of birth, ethnic origin
- Medical information
- Opinions and evaluations of or about an individual
- Religious, political or civil affiliations, where applicable
- Consumer activity
- Personal information does not include
- Business title, address or telephone number of an individual
- Information collected for artistic or literary purposes
- Personal employee information

Personal information does not include

- Business title, address or telephone number of an individual
- Information collected for artistic or literary purposes
- Personal employee information

Personal Information Protection Act (PIPA):

Provincial legislation governing the collection, use and disclosure of personal information and personal employee information by private sector organizations in the province of Alberta. PIPA does not apply to personal health information that is not collected, used, or disclosed for employee management purposes. Personal health information collected, used, or disclosed for other purposes is subject to the provisions of the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

In Alberta, PIPA extends to employee information in the custody or control of private sector organizations. BC's privacy legislation governs the collection, use and disclosure of personal information, excluding employee information.

For personal information under the jurisdiction of PIPEDA, Independent review is provided by the federal Office of the Privacy Commissioner. Similarly, the Information and Privacy Commissioner for Alberta conducts reviews and investigates complaints involving the collection, use or disclosure of personal information by private sector organizations in Alberta

Personal Information Protection and Electronic Documents Act (PIPEDA):

Federal privacy legislation that governs all personal information, including health information, collected, used or disclosed by federal works and by private sector organizations for commercial business transactions in Canada. PIPEDA does not apply to personal employee information in organizations that are not federal works. PIPEDA also does not apply to areas where provincial privacy legislation, such as PIPA, is in force.

For personal information that is collected, used or disclosed by private sector organizations in provinces where no provincial legislation exists to govern how personal information is handled, the federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies.

In provinces with no privacy legislation, or if personal information is transferred across provincial borders, the rules set out in PIPEDA must be followed. PIPEDA only applies to employee information in organizations that are engaged in federal works, undertakings or businesses.

Record:

information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers, and any other information that is written, photographed, recorded or stored in any manner but does not include software or any mechanism that produces records. Software and other mechanisms used to produce records are not considered records for purposes of the legislation.

Records subject to Privacy Legislation:

All records in Canadian Career Partner's custody or control that contain personal information are subject to provincial or federal privacy legislation. Personal information about an individual that was acquired prior to January 1, 2004 is deemed to have been collected with the consent of the individual, and may be used and disclosed by Provident only for the purposes for which the information was collected.

The only basis for refusing an individual's request for access or correction to records may be the exclusions and exceptions set out in the governing legislation. The legislation should always be interpreted with a view to giving an individual as much access as possible to the records requested

Routine disclosure:

When access to a record can be granted without a formal request for access or correction under PIPA or PIPEDA.

Severing:

In a right of access request, separating or hiding information in a document so that the remainder of the document can be disclosed.

Staff:

Employees, Associates, Contractors, and Agents

Third Party:

Organization or person not involved in a transaction or exchange between Provident and another person or party, but who may have an interest. For instance, if a person is requesting access to personal information, anyone whose personal information is documented in the records that is not the person making the request is the third party.

Use:

Personal information employed by Provident for an identified business purpose that is authorized by policy or law.