Privacy and Information Security

1. Purpose

Veren Inc. and its subsidiaries (collectively, "Veren", the "Company" or "we") are committed to safeguarding the Personal Information (as defined herein) entrusted to the Company by all Workers (as defined herein) and members of the public. This Privacy and Information Security Policy (the "Policy") describes how Personal Information will be collected, used, disclosed, and protected by Veren. Veren has established this Policy in order to ensure compliance with legal requirements and to ensure confidence in the Personal Information management practices of the Company. This Policy should be read in conjunction with Veren's Right of Access and Correction Policy, Collection Use and Disclosure of Personal Information Policy and **[the Procedure for Information Handling and Security]**.

2. Scope and Application

This Policy applies to:

- All Workers;
- Any identifiable Personal Information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out Veren functions and activities; and
- All facilities and equipment required to collect, manipulate, transport, transmit, or keep Veren information.

3. Legislative Requirements

Veren has operations in multiple jurisdictions within Canada and in the United States. Throughout the Policy, the most stringent standard has been used to ensure that Veren meets its legislative requirements in all jurisdictions without requiring different policies in each location.

Veren may establish offices or operations in new jurisdictions. This Policy will be reviewed, as needed, to ensure compliance with specific legislative requirements.

Veren may also have Workers operating remotely from various locations throughout North America. Veren will continue to assess whether those situations create new privacy obligations for Veren.

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies in all Canadian provinces except those provinces that have enacted legislation that is deemed to be substantially similar to the federal law. Alberta, British Columbia, and Quebec are the only provinces that have adopted substantially similar legislation to date.

Privacy in each of Veren's locations is governed by the following legislation:

- Alberta: the Alberta Personal Information Protection Act (PIPA)
- Saskatchewan: PIPEDA
- North Dakota: No privacy legislation

- Remote Workers: The privacy legislation applicable to the office or operations the remote Worker is supporting

4. Definitions

"**Applicant**" A Worker who has made a formal request for access to Personal Information or a request for correction under the applicable legislation.

"**Authorized Representative**" Any person who can exercise the rights or powers of a Worker. This includes the right of access to a Worker's Personal Information and the power to provide Consent for Disclosure of such information. This may include:

- a guardian or trustee appointed under legislation, in accordance with the guardianship or trustee order;
- a deceased Worker'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 Worker if the exercise of the right or power relates to the powers or duties conferred by the power of attorney; or
- any person with written authorization from the Worker to act on the Worker's behalf.

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

"**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 Veren for a defined purpose. Consent may be explicit, implied or opt-out, and may be revoked at any time.

"**Contracted Service Provider**" An individual or company, other than a Worker, providing services to Veren under agreement.

"**Control of Records**" A Record is under the control of an organization when the organization has the authority to manage the Record, including restricting, regulating, and administering its use, disclosure or disposition.

"**Custody of Records**" An organization has custody of a Record when the Record is in the possession of the organization.

"***Disclosure***" Making Personal Information in Veren's custody or control available to an external individual or organization, including a contractor.

"**Notification**" An explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of Personal Information. Veren must properly inform and notify individuals and Workers that Personal Information is being collected, and the purposes for which it is being collected.

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

- Name, address, age, gender or gender identity, orientation, family status;
- Educational, criminal, 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; and
- Consumer activity.

Personal Information does not include:

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

"**Personal Worker Information**" Personal Information collected, used, or disclosed for the purposes of establishing, managing, or terminating a Worker relationship.

"**Record**" includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded.

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

"**Third Party**" Organization or person not involved in a transaction or exchange between Veren 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 who is not the person making the request is the third party.

"**Use**" Personal Information employed by Veren for an identified business purpose that is authorized by policy or law.

"**Worker**" All directors, officers, employees, volunteers, consultants and contractors employed by or providing services on behalf of Veren.

Roles and Responsibilities

1. Privacy Officer

The Privacy Officer for Veren is the Senior Vice President, General Counsel and Corporate Secretary.

The responsibilities of the Privacy Officer include:

- identifying privacy compliance issues for Veren;
- ensuring that privacy and security policies and procedures are developed and maintained as necessary;
- ensuring that Workers 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, including Personal Information;
- in consultation with Veren officials as required, responding to requests for access to information, or to correct or amend Personal Information, and facilitating the request process;
- ensuring the overall security and protection of Personal Information in the custody or control of Veren; and
- representing Veren in privacy and information security related matters, dealings with third parties, provincial / state governments, and the federal, provincial, or state regulators, as necessary.

2. Chief Executive Officer

The Chief Executive Officer of the Company appoints the Privacy Officer.

3. Board of Directors

The Board of Directors of the Company reviews and approves the Policy.

4. All Workers

All Workers are responsible for complying with the Policy, including:

- making themselves aware of, and adhering to, access to information and privacy policies and standards;
- accessing, releasing and protecting Personal Information in their custody or control according to the Policy; and
- referring all decisions about collection, use, disclosure, and access that are not clearly directed by the Policy to Veren's Privacy Officer.

5. Contracted Service Providers

Veren is responsible for safeguarding, in accordance with this Policy and its related Procedures, all Personal Information generated by external service providers completing contracted services for Veren. Veren ensures Contracted service providers (e.g., support service providers or business partners) comply with this Policy and its related Procedures.

Privacy Principles

Veren is committed to protecting the privacy of Workers and members of the public. To that end, Veren has implemented a privacy program to meet the following privacy principles.

a. Accountability

Veren is responsible for protecting the confidentiality of Personal Information in its custody or under its control in compliance with the applicable federal, state, or provincial legislation and this Policy.

Veren has identified and designated a Privacy Officer to be responsible for implementing the privacy program and ensuring compliance with applicable federal, state, or provincial legislation and this Policy.

b. Openness

Veren's privacy and security policies and practices are publicly available, support openness and transparency.

c. Collection and Consent

Veren collects Personal Information only for reasonable business purposes and with the Consent of the Worker or Authorized Representative, except where otherwise authorized by applicable federal, state, or provincial legislation.

The least amount of Personal Information is collected, with the highest degree of anonymity, to meet the business purpose. The collection cannot be for a prospective program or activity that does not currently exist, and Personal Information must not be collected "just in case."

When Consent is required, Veren will obtain the Consent of the Worker before collecting the Personal Information. If additional Consent is required for Use and Disclosure, Consent will be obtained from the Worker before the new Use or Disclosure occurs.

d. Identifying Purposes

Veren identifies the purposes for which Personal Information is collected by providing a notification before the collection takes place.

e. Limited Use, Disclosure and Retention

Veren 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 Worker or as authorized by applicable federal, state, or provincial legislation.

f. Accuracy

Veren makes all reasonable efforts to ensure Personal Information collected, used, or disclosed by or on behalf of Veren is accurate and complete.

g. Safeguards

Veren 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.

Veren has also established criteria, standards, and procedures for identifying and managing Personal Information within security zones, and addressing Veren's obligations to protect and secure Personal Information. The goal is to enhance the consistency and quality of Personal Information security at Veren and to support the Privacy Breach Response.

h. Right of Access

Individuals have a right to access Personal Information that Veren holds about them, subject only to limited and specific exceptions authorized by legislation.

Workers who believe there is an error or omission in their Personal Information have a right to request correction or amendment of the information.

6. Compliance Challenges

Workers are encouraged to bring any concerns or issues regarding privacy to the Privacy Officer for discussion and response. Workers may appeal to the Information and Privacy Commissioner for their jurisdiction (or to the similar authorized person in the applicable jurisdiction) to review or investigate Veren's response to the Worker's access to Personal Information request or a request for correction, or any policies or practices they think are not in compliance with applicable federal, state, or provincial legislative requirements.

7. Penalties

Violations of this Policy may result in disciplinary actions up to and including revocation of access to Veren networks and systems, termination of employment or service agreement, and/or legal action.

Reports of violations should be forwarded to the Senior Vice President, General Counsel and Corporate Secretary for follow up.

In cases where local or international laws have been violated, Veren has a responsibility to involve appropriate law enforcement agencies.

For additional provisions and procedures addressing the Company's approach to privacy and information security, see the following procedures:

- Collection, Use and Disclosure of Personal Information
- Information Handling and Security
- Right of Access and Correction

Procedures For Right of Access and Correction

INTRODUCTION

This document should be read in conjunction with Veren's Privacy and Information Security Policy (the "Privacy Policy") and all of the related policies and procedures referenced therein. All capitalized terms used, but not defined, herein shall have the respective meanings set forth in the Privacy Policy.

1. Individual Requests for Access to their Own Information

Requests from Workers to access Personal Information about themselves are handled as a routine release of information.

Formal requests for access to Personal Information that may involve review and Severing must be in writing to Veren's Privacy Officer.

A Worker may request access to another Worker's Personal Information only if they have signed Consent from that Worker or if they can prove they are the Worker's Authorized Representative.

Workers making routine or formal requests may be required to provide enough information to verify their identity and authorize access to the Personal Information. Any such Personal Information provided is used for these purposes only.

Veren will typically respond to formal requests for access to Personal Information within thirty (30) calendar days of receipt of the request. Veren may, however, extend the deadline for response to a formal request for an additional 30 days, or, with the permission of the relevant Privacy Commissioner for a longer period, if:

- The Applicant does not give sufficient detail to enable Veren to identify the requested Record;
- A large amount of Personal Information is requested or must be searched;
- Meeting the time limit would unreasonably interfere with the operations of Veren; or
- More time is needed to consult with another organization, a public body, or a government or an agency of a government of a jurisdiction in Canada before Veren is able to determine whether or not to give the Applicant access to the requested Personal Information.

Veren does not charge Workers for access to their own Personal Information. However, reasonable fees may be charged for reproduction, transcription, or transmission of Personal Information, so long as the Worker is notified before these costs are incurred. A fee for reasonable costs incurred may be charged when responding to complex requests. The Worker will be informed of the fee in advance.

Requested Personal Information will be provided in a form that is generally understandable. Veren will endeavor to explain the meaning of the content, codes and abbreviations included in the Worker's Personal Information to the extent that it is reasonably practical.

In providing an account of Third Parties to whom Veren has disclosed Personal Information about a Worker, Veren will be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed Personal Information about an Worker, Veren will provide a list of organizations to which it is likely to have disclosed information.

Workers are permitted to view either the original Record, or to request a copy of the Record containing their Personal Information, subject to exceptions under applicable law, rule, and regulation. To preserve the integrity of the Record and ensure that documents are not removed from Veren, a Worker wishing to view an original Record containing their Personal Information will do so under the supervision of designated personnel.

2. Exceptions to Right of Access

In certain situations, Veren may not be able to provide a Worker access to all the Personal Information it holds about them.

Veren must not release to the Worker making the request, Personal Information about another Worker without the other Worker's Consent.

Veren must refuse to provide access to Personal Information when it reveals the identity of a Third Party providing an opinion about a Worker unless the Third-Party Consents to the access.

Veren may refuse to provide access to Personal Information:

- if access could reasonably be expected to threaten the life or security of another Worker;
- that is protected by solicitor-client privilege;
- that would reveal confidential commercial information;
- that was collected without the Worker's knowledge or Consent as part of an investigation of a breach of agreement, policy, 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; or
- if Disclosure might result in that type of information no longer being supplied and it is reasonable for Veren to require that type of information for its business purposes.

Veren will always provide access to Personal Information if it is needed because a Worker's life, health, or security is threatened.

If Veren refuses to provide access to Personal Information, the excepted Personal Information is appropriately severed from the record before providing it to the Worker.

Veren will inform the Worker in writing of the refusal or acceptance of any request for Personal Information, the reason(s) for any refusal, and any recourse the Worker may have to challenge Veren's decision.

3. Individual Requests to Correct or Amend Personal Information

Requests from Workers to correct / amend Personal Information about themselves (e.g., change of name or address) are handled as a routine correction of information.

Formal requests to correct or amend Personal Information subject to review must be made in writing to Veren's Privacy Officer. A Worker may request the correction of another Worker's Personal Information only if they have that Worker's signed Consent or they can prove they are the Worker's Authorized Representative.

All formal requests must be accompanied by appropriate documentation to support the request before Veren will amend the Personal Information as required and as appropriate. Generally, Veren will not amend professional opinions that are made by staff that have the competency to make them. If amendments are made, the original Personal Information must not be deleted but retained and marked as incorrect, for example by crossing out. The amended Personal Information may be transmitted to Third Parties, as appropriate.

Veren will typically respond to formal requests for correction of Personal Information within thirty (30) calendar days of receipt of the request.

Veren will inform the Worker in writing of the refusal or acceptance of the request, the reason(s) for the refusal, and any recourse the Worker may have to challenge Veren's decision.

If the Worker is not satisfied with the results of their request, Veren will internally document the issue in the relevant record(s) and provides a response. The existence of the unresolved challenge may be transmitted to Third Parties, as appropriate.

4. Individual Challenges to Request Responses

Workers are encouraged to bring any concerns or issues about responses to requests or compliance with this Policy to Veren's Privacy Officer for discussion and mediation. Workers may also challenge responses in writing to the Information and Privacy Commissioner of the applicable jurisdiction.

Procedures For Collection, Use and Disclosure of Personal Information

This document should be read in conjunction with Veren's Privacy and Information Security Policy (the "Privacy Policy") and all the related policies and procedures referenced therein. All capitalized terms used, but not defined, herein shall have the respective meanings set forth in the Privacy Policy.

1. Collection, Use and Disclosure

1.1 Collection

Veren collects Personal Information with the consent of the Worker in accordance with consent standards (see Section 2.), unless it is for one of the exceptions listed below.

Personal Information can be collected without the consent of the Worker 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 Veren;
- 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 Veren;
- to contact next of kin or friend of an individual who is deceased, ill, or injured;
- to determine the Worker's suitability to receive an honor, award, or similar benefit, including an honorary degree, scholarship or bursary; or
- to conduct a sale, purchase, merger, or amalgamation between Veren and another party, under a restrictive agreement.

1.2 Use and Disclosure

Veren uses and discloses Personal Information only for the following purposes:

- purposes consistent with those to which the Worker consented at the time of collection; or
- purposes for which consent was not required at the time of collection.

Uses and Disclosures of Personal Information for other purposes require the consent of the Worker in accordance with consent standards (see Section 2). However, consent is not required for the Disclosure of 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 support legal counsel in order to represent Veren; or
- to a surviving spouse, partner or relative of a deceased Worker if the Disclosure is reasonable.

1.3 Personal Worker Information

Personal Worker Information collected must be limited to that required to recruit potential Workers, or to manage or terminate existing Workers at Veren ("Worker Management Purposes"). The purposes for collection of Personal Worker Information may include, but are not limited to:

- Worker recruitment, classification, and compensation;
- occupational health and safety;
- performance and conduct evaluation;
- professional development; and
- payroll and benefits administration.

Consent is not required when Personal Worker Information is collected, used, and disclosed for Worker Management Purposes. For all other purposes, Veren will obtain the consent of the Worker using the Consent Form (see Appendix 1).

Whether or not Consent is required, all potential, existing, and past Workers will be notified of the purposes for which their Personal Worker Information is collected, used, and disclosed before the collection, Use, or Disclosure of the Personal Worker Information.

2 Consent and Notification Standards

2.1 Application

When consent is required, Veren will obtain the Consent of the Worker before collecting the Personal Information. If additional Consent is required for Use and Disclosure of Personal Information, Consent will be obtained from the Worker before the new Use or Disclosure occurs.

2.2 Form of Consent

There are three options for determining the appropriate Consent to the gathering, Use, or Disclosure of Personal Information has been obtained by Veren:

- *"Explicit Consent":* The individual is properly informed and explicitly gives permission, either in writing or orally, before action is taken.
- *"Implied or deemed Consent":* Permission is reasonably implied based on the circumstances of the transaction:
    - The individual intentionally and directly releases the Personal Information to the organization; or
    - the nature and purposes of the collection are so clear to the individual that they do not need to be stated or explained.
- *"Opt-out Consent":* An individual is given reasonable opportunity to express their wish to not allow the gathering, Use, or Disclosure of the individual's Personal Information; if no response is given, Consent is assumed.

Explicit Consent is required for collection of all Personal Information from members of the public, which excludes Workers unless specifically authorized by the Privacy Policy.

Explicit Consents contain the following minimal elements:

- an authorization from the Worker or Authorized Representative;
- the purposes for collection, Use or Disclosure;
- identification of the intended users or recipients of the Personal Information;
- an acknowledgement that the individual providing the consent understands the risks of consenting or refusing to consent;
- the effective date and, if any, the expiry date of the consent; and

- a statement that the consent may be revoked by the individual at any time.

Opt-out Consent is only available when dealing with Personal Information limited to name and location or contact information.

2.3 Consent Process

Only the Worker or Authorized Representative can provide Consent by the gathering, Use, or Disclosure of Personal Information.

Veren cannot refuse a service to an Worker if they refuse to give their Consent for the collection of Personal Information beyond what is reasonably required to provide the service.

A Worker may refuse to give Consent for Personal Information to be collected in relation to a specific purpose Veren has identified. In the event that an individual places reasonable conditions on their Consent, Veren must consider whether there is another way the purpose may be achieved without collecting the Personal Information.

A Worker may revoke Consent at any time by notifying Veren. Notification may be in writing or by another form of communication.

2.4 Notification

Veren will ensure the Worker is properly notified of the purposes for collecting their Personal Information before the collection takes place. Notification to the Worker from whom the Personal Information is collected will include:

- the specific purposes for which the Personal Information will be used or disclosed;
- the specific legal authority for the collection of Personal Information; and
- the title, business address and telephone number of the Veren official who can answer questions about the collection of Personal Information.

Veren notifies Workers through the use of appropriate notices, forms, posters, verbal statements, brochures, or other forms of communication.

No notification is required when Personal Information is collected with Implied or deemed Consent.

Procedures For Information Handling and Security

INTRODUCTION

This document should be read in conjunction with Veren's Privacy and Information Security Policy (the "Privacy Policy") and all the related policies and procedures referenced therein. All capitalized terms used, but not defined, herein shall have the respective meanings set forth in the Privacy Policy.

1. Administrative Safeguards

Veren ensures policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained.

The need for confidentiality and security of Personal Information is addressed as part of the conditions of employment for Veren employees, beginning with the recruitment stage, and included as part of job descriptions and contracts. All Workers must be aware of, and appropriately trained on policies and procedures for safeguarding information, including the Appropriate IS Usage Policy. Confidentiality Policy, Disclosure Policy and Account Management Policy and Practices.

All Veren Workers that collect, use, disclose or have access to confidential information as part of the performance of their duties must sign the Confidentiality Policy and Disclosure Policy.

Before implementing proposed new administrative practices or information systems that will change or significantly affect the collection, Use and Disclosure of Personal Information, Veren completes an assessment that describes how the new initiative will affect privacy, and what measures Veren will put in place to mitigate risks to privacy.

Veren Workers report all violations and breaches of information security as soon as possible to Veren's Privacy Officer. This enables the Privacy Officer to take corrective action to resolve the immediate problem and minimize the risk of future occurrence.

2. Physical Safeguards

All Veren Records, both on-site and off-site, are held and stored in an organized, safe, and secure manner in accordance with information security standards.

Appropriate fire detection and extinguishing devices are in areas where Personal Information is stored.

Veren Records are not accessible by unauthorized persons. In areas where unauthorized persons are present, measures will be taken to ensure that files are not left unattended or accessible.

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.

All servers and equipment storing electronic Personal Information are secured by locked cabinets or rooms within Veren when not under direct supervision by staff.

Veren Records or equipment holding Personal Information (e.g., laptop computers) may not be left unattended in a vehicle for any significant length of time, even if the vehicle is locked.

Appropriate measures are taken to control the distribution of keys or pass codes, and to ensure they are returned or changed after employment or association with Veren has ended.

Confidential information will be treated with sensitivity. Workers will take care when sharing information if conversations can be overheard or intercepted by unauthorized individuals.

Confidential, restricted, or sensitive information that is transmitted by mail or courier will be sealed, marked as confidential, and directed to the attention of the authorized recipient.

Veren Workers will verify the identity and credentials of courier services used for the transportation of Personal Information.

Information that is not confidential or sensitive in nature will be recycled. Confidential or sensitive information is destroyed by shredding. Destruction will be documented by listing the Records and / or files to be destroyed, the date of destruction, and an employee's signature to confirm that the destruction occurred.

All confidential or sensitive information stored electronically will be deleted by a third party 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) will be destroyed. Destruction will be documented by listing the Records and / or files to be destroyed, the date of destruction, and a certificate will be issued by the third party to confirm that the destruction occurred.

The retention period for Personal Information is set according to the business requirements of Veren, which is further described in the Records Management and Retention Policy. Personal Information that was used to make decisions about a Worker will be kept for at least one year after the decision has been made.

Information will not be retained for longer than is reasonably necessary to fulfill the purpose for which the information was collected.

3. Technical Safeguards

Firewalls, intrusion detection software, or other technical means to protect internal Veren networks carrying identifiable Personal Information are in place to prevent unauthorized use and malicious software.

Access to data and application systems to Personal Information is limited by each Worker's functional role and need to know.

Workers of Veren access and use information systems under their assigned User ID. The use of another person's assigned User ID is prohibited..

Access to Veren information systems is controlled and password/passphrase protected. Passwords are kept confidential at all times and will not be written down, posted publicly, or shared with other Wokers. Passwords/passphrases will be changed on a regular schedule. If a computer is left unattended, it will be protected against unauthorized access by manual or automated logout requiring authentication to re-enter the system.

Equipment, such as fax machines and printers that may be used to send or receive confidential information are located in a secure area. Whenever possible Workers will use preprogrammed numbers to send transmissions and will review the numbers every six (6) months to ensure they are still accurate.

All transmissions will be sent with a cover sheet that indicates the information being sent is confidential. Reasonable steps are taken to confirm that confidential information transmitted is sent to a recipient with a secure fax machine, printer or device. See Appendix 2.

Personal Information is not permitted to be sent by e-mail or transmitted over the internet or external networks without the use of appropriate security safeguards, such as encryption and authentication. E-mail messages must also contain a confidentiality notification. See Appendix 2.

To detect unauthorized access and prevent modification or misuse of user data in applications, systems may be monitored to ensure conformity to access policies and standards. Appropriate security controls, such as event logs, will be implemented and reviewed as required.

Computer systems that hold critical or sensitive information will be backed up daily. Backed up information is stored in a secure environment off-site. Information that is intended for long-term storage on external electronic media (e.g., external hard drive or cloud storage) will be reviewed on an annual basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

4. Security in Contracting

Veren ensures contracted service providers or business partners comply with Veren's Privacy Policy and other related policies.

If a Contracted Service Provider requires access to Personal Information or systems affecting the security of Personal Information as part of their services, the contractor must sign a privacy and security agreement outlining the conditions of access (Appendix 1), in addition to the Privacy Policy.

Until a contract detailing explicit information security provisions has been executed, the Contracted Service Provider is not given access to premises or systems containing confidential business or Personal Information of Veren.

Information security provisions outlined in contracts with contracted service providers meet or exceed the standards set out in Veren's information security related policies and procedures. Any related Contracted Service Provider information security and privacy policies should be made available to Veren upon request, including any updates or revisions that occur after execution of the contract.

Contracts with Service Providers that have access to Veren information assets and systems include provisions that protect Veren operations from circumstances where the information assets or systems may be compromised. In order to mitigate these situations, disaster recovery and system backup provisions must be included in all agreements, to a standard that meets or exceeds that of Veren.

Contracts with Service Providers include provisions for destroying or returning all Veren 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.

All employees of Contracted Service Providers who have exposure to and use Veren information assets and systems sign a Confidentiality (non-disclosure) Oath (Appendix 1). Contracted Service Providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of Veren information.

Contracted Service Providers immediately report breaches of confidentiality and privacy to Veren's Privacy Officer.

To ensure compliance with contracted provisions for information security, Veren:

- requests Contract Service Providers sign an acknowledgement that they have received, read, and will comply with any Veren information security policies they are bound to follow under contract; and
- actively monitors Contracted Service Providers with access to information assets or systems for inappropriate access or use and to ensure compliance with contract security provisions.

Veren retains the right to inspect the premises and security practices of Contracted Service Providers without notice to ensure compliance with contract provisions and stated policies.

For Canadian operations, Veren avoids using Contracted Service Providers that require the storage or transmission of Personal Information outside of Canada. If they are retained, Veren ensures that they meet the same standards of security and compliance that are required of Canadian service providers, in order to fulfill the legislative requirement to prevent unauthorized collection, Use, access, retention, destruction and Disclosure of Personal Information. Personal Information related to US operations may be stored or transmitted within Canada or the United States.

5. Information Security Classification

5.1 Security Classification

Information is classified according to the degree of harm that may result from unauthorized access, loss, or modification. All information is classified as “Restricted”, “Confidential”, “Internal”, or “Public” in accordance with the levels identified in the Information Security Classification and Standards Table in Appendix 3.

5.2 Security Zones

Physical spaces and areas and logical areas within electronic systems and networks are identified as having the status of one of four security zones, based on the functionality of the area:

RESTRICTED: Used infrequently by a subset of authorized individuals with special status for storing, transmitting, and accessing information on a limited basis;

INTERNAL: Used regularly by authorized individuals working within the zone for storing accessing and transmitting information among them;

EXTERNAL: Used regularly by a controlled number of unauthorized and authorized individuals for accessing, and transmitting information among them within the zone; or

PUBLIC: Used regularly by both authorized and unauthorized individuals for other, uncontrolled purposes.

Veren maintains standards to ensure the integrity of each zone, including definition of perimeters, barriers to access, and security practices and equipment within the zone. Physical Security Zones Requirements Table and the Network Security Zones Requirements Table in Appendix 5 provide details of standards required for each zone.

6. Privacy Breach Response

6.1 Principles

A breach is an unauthorized Disclosure, Use, destruction, loss, removal, modification, or interruption in the availability of information. Veren has established and prescribed procedures for reporting, investigation, and follow up of information security breaches as part of its obligations to protect and secure Personal Information.

The gravity of the incident determines the nature of the response, reporting structure, remedial action, and the investigation process. Gravity is based on the security classification of the information and the source of the incident.

Veren uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of persons being investigated, including:

- keeping investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;
- using surveillance or monitoring data to establish past or current actions on an as-needed basis;
- disclosing information as needed to establish or confirm the veracity of information or statements; and
- informing participants of their status and the progress of the investigation as fully and quickly as possible so long as it does not jeopardize the integrity of the investigation.

The privacy breach investigation is an administrative rather than a disciplinary process. Once the report is delivered, it is the responsibility of Veren's Human Resources team to consult with leadership to determine the appropriate disciplinary action.

All Workers of Veren have a responsibility to recognize privacy breaches and report them to the Privacy Officer.

6.2 Privacy Breach Response Guidelines and Procedures

Privacy Breach Response Procedures

Step 1: Identifying and Reporting of Breach

When an information security breach has been discovered, determine the level of the incident, and follow the timelines in the Privacy Breach Response ("PBR") Table. The levels correspond to the gravity of the breach, which is determined by the classification of the information (see Information Security Classification Table) and the source of the breach.

Level 1 Low: The information that was breached is:

- Classified as Internal use only ("I"); the source or threat of the breach or violation is internal (a Worker or affiliate) or external (someone outside Veren); or,
- Classified as Confidential ("C"); the source or threat is internal and involves Workers or affiliates who do not know the people identified in the information.

Level 2 High: The information that was breached is:

- Classified as Confidential ("C"); the source or threat is external, involving persons who are not Workers or affiliates, or internal, if it is reasonably likely that the persons involved are Workers or affiliates who know the people identified in the information; or,
- Classified as Restricted ("R"); the source or threat is internal only.

Level 3 Critical: The information that was breached is:

- Classified as Restricted ("R"); the source or threat is a person outside of Veren.

When a breach level is identified, report the incident to the appropriate Leader and the Privacy Officer ("PO") within the PBR Table Step 1 timelines. If unable to determine the level of the breach, contact the PO immediately.

The reporter of the breach and the PO complete Section 1 and 2 of the Privacy Breach Response (PBR) Form (Appendix 6) by recording the exact timelines and a preliminary of the breach.

Step 2: Containing the Breach:

At this stage, the PO will confirm the level and status of the breach and use all available means and to ensure that Veren information in the custody of unauthorized parties is returned to Veren or destroyed irrevocably within the timelines established in the PBR Table Step 2.

Depending on the level of the breach, IS, Veren leadership and the police are informed.

The PO will document the incident as a breach case using the PBR Form, identifying the potential harm, recording additional information about the breach and the containment efforts.

Step 3: Subject Notification:

For all Level 2 or 3 privacy breaches, notify the Office of the Information and Privacy Commissioner's Office ("OIPC") and consult with them about notifying subjects of the breach based on the information known to this point. Notification may not be advisable, feasible or necessary, or may be limited by several factors:

- The potential harms are negligible;
- Notification may unduly harm the subject;
- Subject contact information is unknown; and
- The number of subjects affected is prohibitively large.

Based on the OIPC's decision, identify and implement an appropriate method for notifying subjects:

- Direct contact with each subject;
- Direct contact with select subjects;
- Announcement and request for contact; and
- Other methods.

Within the timelines set in the PBR Table Step 3, the PO Records the consultations and notification actions and status in PBR Form.

Step 4: Investigation:

Open the investigation by identifying individuals or data that establish the facts of the incident (who, what, where, when and why). Individuals consulted could include the subjects, the source of the breach, experts, or witnesses. Data sources could include access logs, surveillance recordings, storage, and transmission logs, etc.

Individuals consulted will be asked not to communicate with other subjects, co-workers, or the public during the investigation.

Record the investigative actions and dates in PBR Form following the timelines set in PBR Table Step 4.

Step 5: Report and Follow up:

In a report in PBR Form, within the PBR Table Step 5 timelines, determine which necessary facts have been established and which have not or cannot be established, and whether policy was intentionally or unintentionally violated. Identify any changes to the assessment of harms and make recommendations on the actions required by Veren to mitigate the harms and to prevent similar breaches from recurring.

The PO does not recommend any actions regarding Worker discipline or termination of employment but may identify an individual as a continuing threat to the security of Personal Information.

Record what follow up actions are planned and the dates they are or will be completed.

Step 6: Authorization and Review:

Once the full report is completed, it is provided to relevant leadership for review. This may include immediate supervisors of Workers involved or IS leadership. After review of the report, they may ask for clarifications about scope and findings, and document their review by signature and date.

The investigator signs and dates the completed report.

Subjects may be notified of the findings based on the previous notification actions and decisions, but other individuals involved in the breach only if it is considered necessary to prevent harm.

Level	Gravity Criteria		Time from detection	Response	Responsibility
	Class	***Source of Breach***			
1 **Low**	I C	Internal and external Internal, if subject not known to source	2 hrs.	Step 1: Report to Privacy Officer	Staff
			16 hrs.	Step 2: 1) Confirm breach 2) Contain breach/retrieve information 3) IS breach, consult with IS Administrator	PO
			20 days	Step 3: 1) Inform, consult with OIPC on response, notification	PO. OIPC
				Step 4: Investigate	PO
				Step 5: Investigative report to: 1) PO 2) Executive	PO
2 **High**	C C R	External Internal, if subject known to source Internal	1 hr.	Step 1: Report to Privacy Officer	Staff
			3 hrs.	Step 2: 1) Confirm breach 2) Contain breach/retrieve information 3) IS breach, consult with IS Administrator 4) Inform Executive	PO
			24 hrs.	Step 3: 1) Inform, consult with OIPC on response, notification 2) Inform subject based on consultations	PO, OIPC
			14 days	Step 4: Investigate	PO
				Step 5: Investigative report to: 1) Executive 2) Subject, if notified, on basic findings	PO
3 **Critical**	R	External	Immediately	Step 1: Report to Manager, PO	Staff
			1 hr.	Step 2: 1) Confirm breach 2) Contain breach/retrieve information 3) Inform Executive 4) IT breach, consult with IT Administrator 5) Inform Police on potential criminal or public safety concerns	PO
			1 hr.	Step 3: 1) Inform, consult with OIPC on response, notification 2) Consult Police, if required 3) Inform subject based on consultations	PO, OIPC, Police
			3 days	Step 4: Investigate/cooperate with Police	PO, Police
				Step 5: Investigative report to: 1) Executive 2) Subject, if notified, on basic findings	PO

APPENDIX 1: PRIVACY AND SECURITY AGREEMENT

Privacy and Security Agreement

Between

VEREN

and

[INSERT NAME]

((hereinafter referred to as "**Service Provider**")

1. Definitions

1.1. Information Security Measures

Equipment, facilities, or other technical, administrative, and physical security measures that are implemented to protect the confidentiality and integrity of Service Information (as defined herein) or any other Veren information that may be affected by **[SERVICE PROVIDER]**'s access to the Service Information.

1.2. Representatives

"Representatives" means any directors, officers, employees, partners, associates, agents, or other authorized persons of **[SERVICE PROVIDER]**.

1.3. Service Information

"Service Information" means any and all of the following information disclosed to [SERVICE PROVIDER] or Representatives by Veren:

(a) financial information, including but not limited to, assets, properties, debts, volume of purchases for sales or other financial data, whether related to Veren generally or to particular products, services, geographic area, or time;

(b) inquiry process information, including but not limited to, Records at issue, draft orders, correspondence, and submissions relating to the inquiry process.

(c) personnel information, including but not limited to, employees' personal or medical histories, compensation, or other terms of employment, actual or proposed promotions, hiring's, resignations, disciplinary actions, terminations, or reasons therefore, training methods, performance, or other employee information;

(d) technical information, including but not limited to, any and all methodologies, procedures, processes, specialized knowledge, formulas, innovations, and inventions (whether patented or not), instructions, descriptions, studies, reports, test results, computer programs (including computer data, computer software and applications), computer systems, and specialized techniques; and

(e) any information, documents, reports, and materials belonging to Veren, its agents, subcontractors, and employees and which [SERVICE PROVIDER] receives from Veren and from any of Veren 's affiliates in connection with the operation of this agreement.

Service Information includes all such information, whether written, electronic, magnetic, or transmitted orally, and any reports, extracts, notes, memoranda, analyses, compilations, studies, or other documents which contains or otherwise reflects such information and any copies or reproductions thereof.

1.4. Services

"Services" means the services set out in the attached Schedule A and which are provided by **[SERVICE PROVIDER]** to Veren pursuant to the _____ agreement dated _____.

2. Veren Ownership and Control of Information

[SERVICE PROVIDER] acknowledges and agrees that all Service Information made available to **[SERVICE PROVIDER]** is the property and under the control of Veren and shall remain the sole property of Veren. **[SERVICE PROVIDER]** acknowledges and agrees that the Service Information is being disclosed to **[SERVICE PROVIDER]** strictly on a Service basis and under a relationship of utmost confidence and trust.

[SERVICE PROVIDER] and Veren agree that the collection, use, disclosure, security, storage and disposal of Service Information and all other information exchanged between Veren and **[SERVICE PROVIDER]** pursuant to this Agreement is subject to the Personal Information Protection Act Alberta and other provincial or federal laws applicable to Veren.

3. Business Reasons for Access

[SERVICE PROVIDER] shall limit its access to Service Information that is required to complete the Services. A description of the Service Information that may be required by **[SERVICE PROVIDER]** and the business reason for accessing this information is included in Schedule A of this Agreement.

4. Option A: Compliance with VEREN Policy

[SERVICE PROVIDER] shall comply with all Veren Policies. Veren shall provide to **[SERVICE PROVIDER]** a copy of all Veren Policies to which [SERVICE PROVIDER] must comply with including, but not limited to, Veren policies relating to the following:

(a) collection, use, and disclosure of Veren information

(b) right of access and correction of Veren information

(c) Privacy Impact Assessments and information security reviews of Veren information and third-party handling systems and procedures

(d) technical and physical protection of Veren information and resources, including:

i. Information storage and handling

ii. user access management

iii. system audit controls

iv. network security

v. equipment and media security

vi. information classification, retention, and destruction

vii. systems backup and recovery

viii. information exchange and electronic mail

ix. personnel security and screening

x. information security training of personnel

xi. information security incidents procedures

By executing this Agreement, **[SERVICE PROVIDER]** acknowledges receipt of the Veren Policies.

Veren shall have the right to amend the Veren policies at any time and [SERVICE PROVIDER] shall comply with such amended Veren Policies immediately upon being provided with notice of the amendment.

Or Option B: Demonstration of compliance with [SERVICE PROVIDER] Policy

[SERVICE PROVIDER] shall demonstrate compliance with all its policies, as Veren has reviewed all **[SERVICE PROVIDER]** policies and approved them as sufficient in meeting the same standards and requirements as Veren's own Policies. **[SERVICE PROVIDER]** shall provide to Veren a copy of all **[SERVICE PROVIDER]** Policies to which **[SERVICE PROVIDER]** must comply including, but not limited to, **[SERVICE PROVIDER]** policies relating to the following:

(a) collection, use, and disclosure of Veren information

(b) right of access and correction of Veren information

(c) technical and physical protection of Veren information and resources, including:

i. information storage and handling

ii. user access management

iii. system audit controls

iv. network security

v. equipment and media security

vi. information classification, retention, and destruction

vii. systems backup and recovery

viii. information exchange and electronic mail

ix. personnel security and screening

x. information security training of personnel

xi. information security incidents procedures

5. Information Security Measures

[SERVICE PROVIDER] shall use its best efforts to implement all information security measures required to comply with this Agreement. If and when Veren believes, acting reasonably, that **[SERVICE PROVIDER]**'s and/or Representative's information security measures are deficient and represent an undue risk to the security of the Service Information or other Veren information, Veren may make a request in writing for **[SERVICE PROVIDER]** to change, modify, or add to such measures. Within (5) days of receipt of this request, **[SERVICE PROVIDER**], at its own expense, shall change or modify its information security measures to comply with this request.

6. Information Security Breaches

In compliance with Veren Policies, **[SERVICE PROVIDER**] shall notify Veren immediately of any breach of information security affecting the service information, including unauthorized disclosure, use, destruction, loss, removal, modification, or interruption in the availability of service information, whether accidental or as the result of a deliberate act. Veren will direct and conduct the breach investigation and will have access to any of **[SERVICE PROVIDER]'**s and/or its Representative's information systems, equipment, facilities, and personnel affecting the Service Information and relevant Records required to complete the breach investigation.

7. Disclosure and Reproduction

Except as necessary to perform the Services, **[SERVICE PROVIDER**] and its respective Representatives shall not disclose, copy, or otherwise reproduce any of the Service Information or part of any of the Service Information, or any reports, extracts, notes, memoranda, or other Records in respect thereof, without the prior written consent of Veren.

8. Return or Destruction of Service Information

[SERVICE PROVIDER] and its respective Representatives shall not copy or otherwise reproduce any of the Service Information or part of any of the Service Information, or any reports, extracts, notes, memoranda or other Records in respect thereof, without the prior written consent of Veren.

At any time upon the written request of Veren, or at the termination of this contract, **[SERVICE PROVIDER]** shall immediately return to Veren or shall have destroyed any and all Service Information and shall not retain any copies or other reproductions thereof. All Service Information returned by **[SERVICE PROVIDER]** or the Representative to Veren must be in a format that is readable by Veren. Furthermore**, [SERVICE PROVIDER]** shall, upon request, provide written confirmation to Veren that the terms and conditions of this section have been complied with.

9. Inspection without Notice

Veren at its discretion shall have the right to make inspections, without notice, of **[SERVICE PROVIDER]**'s and/or its Representative's information systems, equipment, facilities, affecting the Service Information and relevant Records to ensure appropriate technical, administrative, and physical security measures are being taken to protect the Service Information or other Veren information in compliance with this agreement.

10. Termination of Access to Service Information

Except where there is a statutory or legal compulsion to disclose the Service Information, **[SERVICE PROVIDER]** agrees that Veren is not obligated to provide **[SERVICE PROVIDER]** and/or its Representatives with any Service Information. Veren shall have the right to cease providing Service Information to **[SERVICE PROVIDER]** and/or its Representatives at any time and for any reason.

11. Compliance by Representatives

[SERVICE PROVIDER] may disclose Service Information to a Representative of **[SERVICE PROVIDER]** who has a need to know the Service Information according to the business reasons in Schedule A. [SERVICE PROVIDER] will implement personnel security and screening for its Representatives to a standard equal to or exceeding those policies and standards in place for Veren employees or according to [SERVICE PROVIDER] standards approved by Veren. [SERVICE PROVIDER] shall, before disclosing any Service Information to any Representative, use its best efforts to ensure that the terms and conditions of this Agreement are and will be fully complied with by any such Representative, including obtaining an agreement in writing of such Representative that he will keep such confidential information in strict confidence and that such Representative shall be bound by all terms and conditions of this Agreement.

At the request of Veren, the Service Provider agrees to provide Veren with a list of all Representatives to whom Service Information has been provided and evidence that the Representatives have agreed to be bound by the

terms and conditions of this Agreement. The Service Provider agrees that it shall be liable and responsible for any breach of this Agreement by its respective Representatives.

12. Use of Subcontractors

[SERVICE PROVIDER] shall not allow any person subcontracted to perform the Services to collect, use, disclose, or otherwise access the Service Information, without the prior written consent of Veren.

13. Liability and Indemnification

Without limitation and in addition to any other rights of Veren against **[SERVICE PROVIDER]** or its Representatives arising by reason of any breach of this Agreement, **[SERVICE PROVIDER]** shall:

(a) be liable to Veren for any and all losses, costs, damages, and expenses whatsoever, including legal, accounting, and other professional costs, expenses, fees and disbursements, legal fees to be determined on a solicitor and his own client basis, which Veren may suffer, sustain, pay, or incur; and

(b) indemnify and hold Veren harmless against all actions, proceedings, claims, demands, losses, costs, damages, and expenses whatsoever, which may be brought against or suffered by it or which it may sustain, pay, or incur;

which are judicially established to result or arise, directly or indirectly, from disclosure or access to all or any part of the Service Information contrary to the provisions hereof or any other breach of this Agreement by [SERVICE PROVIDER] or any of its Representatives.

14. Legal Obligation to Disclose

If **[SERVICE PROVIDER]** or its Representative is or becomes legally compelled, by subpoena, warrant, court order, statutory requests, or other legal process to disclose any of the Service Information, **[SERVICE PROVIDER]** shall provide Veren with immediate written notice of this compulsion to allow Veren to seek a protective order or other appropriate remedy. If such protective order or remedy is not obtained, **[SERVICE PROVIDER**] or the Representative shall:

(a) provide only that part of the Service Information which is legally required;

(b) use its best efforts to assure that the Service Information will be remain secure and confidential; and

(c) immediately provide Veren with copies of the request for the Service Information and all Service Information that was disclosed.

15. Relationship to other Agreements

This Agreement is supplementary and in addition to the Contract and any other contractual obligations that may exist between **[SERVICE PROVIDER]** and Veren and can only be amended by agreement in writing executed by the parties.

VEREN	**[SERVICE PROVIDER]**
Signature	Signature
Print Name, Title	**Print Name, Title**

SCHEDULE "A"

Service Activity	Service Information	Type of Access
Provision of Information Technology Services	All	Prohibited from accessing any Service Information, but may have unsupervised physical access to any documents, files, computers, servers while completing services.

APPENDIX 2: SECURITY OF ELECTRONIC TRANSMISSIONS

All Transmissions

Limit transmission to circumstances where it is immediately necessary for time-sensitive or functional reasons and to the least amount of information possible.

All e-mail signatures include the following statement:

If you have received this email in error, just let me know by return email so that we can make sure it doesn't happen again. In the meantime, please do not disclose, copy, distribute or use this e-mail or its attachments. Thank You.

All facsimile transmissions must be accompanied by the following statement:

If you have received this fax in error, just let me know by emailing me (employee@VEREN.com) or calling (403-294-xxxx) so we can make sure it doesn't happen again. In the meantime, please do not disclose, copy, distribute or use this fax. Thank You.

Veren Workers will only send or forward very large documents or attachments when absolutely necessary.

Veren will protect data awaiting output to a level consistent with its sensitivity. Only those authorized should see the data spooled.

Electronic Mail

Do not transmit by e-mail over a service other than the Company e-mail service (e.g., gmail).

Remove all personal identifiers from the message if possible.

Do not transmit identifiable Personal Information by e-mail to an external or public zone unless the information is secured by encryption.

Do not include identifiers or Personal Information in the subject header of the e-mail.

Verify all addresses as correct before sending messages.

Develop, update and use e-mail addresses from address book.

Request notification of receipt.

Veren Workers 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.

Transmissions via printer/ computer/ fax equipment

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 transmission, the responsibility to confirm secure receipt of the information lies with the sender.

.

To ensure accuracy in connecting to the correct receiver, confirm the contact number/e-mail by visual check on the computer / printer / fax machine display. For frequently contacted receivers, use the automatic

programming feature to minimize the risk of sending information to an incorrect receiver. For example, for automatic faxing by computer, use a fax table for automatic dialing of numbers.

Where possible, use available security features on the equipment, i.e. confidential mailboxes, to ensure the confidentiality of information.

Print out and check the equipment logs after transmission to verify that documents were received at the correct number.

If it is determined that the transmission was received by a wrong number / recipient, contact the recipient and ask them to return or destroy the documents; and retain copies of all information sent.

Report the incident as an information security breach to the Privacy Officer.

Inspections of E-mail Messages

Veren may view, monitor or inspect any messages sent or received using the Veren system in order to:

- investigate information security incidents
- support an urgent, time-sensitive action
- maintain Veren information systems
- comply with a court order or statutory requirement

Where access to e-mail is deemed necessary, Veren 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 Veren policy.

Filing and Retention of E-mail messages

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

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

APPENDIX 3: INFORMATION SECURITY CLASSIFICATION TABLE

Class	***Harm***	***Information Type***	***Security Zones****	***Copying Destruction***
Restricted **R**	• Harm to operations of facilities or security systems • Immediate harm to health and safety of the public, clients, or staff • Loss of essential Records required in case of emergency	• Information describing security systems, access codes, etc. • Personal Information that would likely cause or allow a person to harm themselves or specific staff, or clients • Information that would allow access to assets of over $10,000 • Essential Records or back-up of essential Records	*Network:* Restricted *Physical:* Restricted	Copying only for backup Supervised on-site shredding or data wiping and destruction logged
Confidential **C**	• Harm to privacy of individuals and staff • Financial loss for Veren or third parties • Damage or loss to Veren assets • Damage to Veren credibility or service integrity • Legislative sanctions • Loss of source record and accountability for decisions	• All Personal Information • Worker information • Information given in confidence or under privilege • Financial accounts access, approval and location information • Third party business information • Deliberations, investigations, advice, decisions • Security audit tools	*Network:* Internal preferred; External by approval *Physical:* Internal preferred; External by approval;	Copying only for backup or when access to original impractical; destroy immediately after use Confidential shredding or data wiping and destruction logged
Internal Use **I**	Loss of source record and accountability	• Staff internal 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;	No restrictions Destruction logged
Public **P**	No identified harms	• Published materials such as pamphlets, newsletter, annual reports • Public information such as directories or web sites	No restrictions	No restrictions

Trusted User: a staff member, affiliate, or third party accessing a Veren network, resource, or building in compliance with Veren security policy and under agreement. Public User: a user not under Veren policy or agreement

APPENDIX 4: SECURITY ZONES TABES

Physical Security Zones Requirements Table

Security Zone	Requirements			
	Authorization	***Barriers to Zone***	***Environment***	***Monitoring***
RESTRICTED *Server rooms, HR Records areas*	• Approved trusted user by function Unauthorized trusted user case-based by authorized person • No public access	• Area only accessed only from Internal zone • Locked and accessible to authorized persons only with ID • Unauthorized visitors accompanied by authorized persons	Enhanced environmental standard	Staff or CCTV surveillance All access logged
INTERNAL *Admin/technical areas, Front desks/reception areas, Individual offices*	• Approved trusted user by function • Unauthorized trusted user by context • Public access case-based by authorized person	• Areas accessed from External or Public Zones • Locked and restricted to authorized persons with ID • Public visitors accompanied by authorized persons • Sound barriers	Normal standard	Staff surveillance Non-authorized access logged
EXTERNAL *Individual offices, Off-sites workplaces: (staff cars/homes, public spaces) Waiting areas*	• Trusted and Public user by context	• Areas accessed from Public or Internal Zones • Locked areas or containers; marked and supervised boundaries • Public visitors unaccompanied but without access to information • Visual access to information by others in area controlled • Low verbal communication	Normal standard	Unlocked areas under staff surveillance Locked entrances to public areas under electronic surveillance
PUBLIC *All other areas*	None	None	May be uncontrolled	

Trusted User: a staff member, affiliate, or third party accessing a Veren network, resource, or building in compliance with Veren security policy and under agreement. Public User: a user not under Veren policy or agreement.

Network Security Zones Requirements Table

Security Zone	**Requirements**					
	User	***Connection***	***Firewall Barriers***	***Zone Authentication***	***Encryption***	***Equipment***
RESTRICTED	Restricted	Internal to LAN/dedicated line		2 factor		
INTERNAL						
Status 1	Trusted	Internal to LAN/dedicated line	Internal DMZ	1 factor	None	Veren
Status 2	Trusted	Ext. via internet	External, Internal DMZ	1 factor	Strong	Veren /External
	Public		No Access			
EXTERNAL	Trusted	Ext. internet to Extranet	External DMZ	2 factor	Strong	Veren /External
	Public		No Access			
PUBLIC	Public		Full Access			

Trusted User: a staff member, affiliate, or third party accessing a Veren network, resource, or building in compliance with Veren security policy and under agreement. Public User: a user not under Veren policy or agreement

APPENDIX 5: PRIVACY BREACH RESPONSE FORM

Privacy Breach Investigation Report		
1. BASIC INFORMATION		
Location	**Occurred Date::**	**Time:**
Responded to:	**Reported Date**	**Time:**
Person(s) involved in Breach:		
2. DESCRIBE THE INCIDENT		
3. WITNESS ACOUNTS		
4. CONTAINMENT		
A breach is contained when: o No further information will be disclosed to or accessed by unauthorized parties from the source, and o Records have been recovered with assurances that no further copies have been made or distributed.		
5. PERSONAL INFORMATION		
Describe the Personal Information involved. Include the extent or volume of the information, the data elements, the relative sensitivity of the information, and the form or format of the information (i.e., electronic		

6. RISK ASSESSMENT

Assess whether the risk to Workers from the breach is low, medium, or high, based on a) the degree of potential harm to the Worker, and (b) the probability that the harm will occur. Identify and briefly describe the following types of harm.

7. SECURITY AT TIME OF BREACH

Describe the applicable security measures and policies and how well they were implemented at the time of the incident.

a. Physical threat(e.g., harassment, self-harm)

b. Hurt, humiliation, damage to reputation;

c. Financial or property loss (from e.g. account hacking, identity theft)

d. Loss of business or employment opportunity

8. ROOT CAUSES

Pinpoint the root cause or causes that led to the breach: was if an isolated incident unlikely to be duplicated or an ongoing or systematic cause that could lead to further incidents.

9. NOTIFICATIONS

Regulator	**Notified by whom:**	**Date:**	**Time:**
Instructions Received			
Other's Notified Names	**Notified by whom:**	**Date:**	**Time:**
Persons Affected:	**Notified by whom:**	**Date:**	**Time:**

To be determined with the Privacy Officer. If not, state rationale:

10. RECOMMENDATIONS FOR PREVENTION

11. ACTIONS TAKEN

12. INESTIGATOR SIGNATURE		
Investigation and Title	Signature	Date
Investigation Stakeholder	Signature	Date
Investigation Stakeholder	Signature	Date