yukon energy

#2 Miles Canyon Road
Box 5920, Whitehorse
Yukon Y1A 6S7
yukonenergy.ca

December 23, 2020

Yukon Information and Privacy Commissioner
3162 Third Avenue, Main Floor
Whitehorse, Yukon Y1A 16E

Delivered by email: info@yukonombudsman.ca

To Whom It May Concern,

Re: Yukon Energy MyAccount Customer Portal

On January 4, 2021, Yukon Energy Corporation (Yukon Energy) will implement an online customer service portal called MyAccount to allow our electricity distribution customers to access account billing information and to make account payments online.

This type of online service has been repeatedly requested by our customers and a common self-serve option provided by other electric utilities across Canada to their customers. MyAccount is configured as a one-way communication from Yukon Energy's existing billing system to the portal. At no time do our customers or the public have access to our billing system.

While Yukon Energy is not identified as a Yukon government department in the government's General Administration Manual (GAM), we have completed our due diligence by completing a *Security Threat Risk Assessment* and *Privacy Impact Assessment* for the MyAccount portal before its scheduled launch.

Attached are those materials for your information.

Kind regards,

Stephanie Cunha
Manager, Communications and Customer Service

Cc: Ed Mollard, Yukon Energy Privacy Officer;
Jeff Sunstrum, Director, Corporate Information Management, Yukon Government

Privacy Impact Assessment:

Yukon Energy Corporation MyAccount *Project*

Date: December 18, 2020

Document Control and Reviews

Document Control

Date	Author	Version	Change Reference
December 18, 2020	Stephanie Cunha	1	Original

Reviews

Date	File Name / Version #	Reviewed by
December 18, 2020	1	Ed Mollard, Yukon Energy Privacy Officer

Note: It is recommended you send your PIA to the department's Privacy Officer for review.

0.1 Policies, Forms and Reports (PIA Manual reference: 5.1 Collecting information and supporting documentation)

Parties Involved	Role
Yukon Energy Corporation	Supplier of a regulated utility (electricity) to approximately 2,200 residents and businesses in the Yukon Territory
The Yukon Electrical Company Limited (an ATCO company)	Developer and service provider of Yukon Energy's billing system, ATCO CIS, and the MyAccount system. Yukon Electrical is also a supplier of a regulated utility (electricity) to approximately 19,000 residents and businesses in the Yukon Territory

Policy Name	Hyperlink or Appendix number
CA – 001	Yukon Energy Records Management Policy – Attachment # 4
CA – 003	Yukon Energy Access to Information and Protection of Privacy Act Policy – Attachment # 7
CA – 004	Yukon Energy Personal Information Privacy Policy for Customers – Attachment # 8

Document Name	Hyperlink or Appendix number
Yukon Energy Terms of Use for the My Account Portal	Attachment #1
Security Threat Risk Assessment for the Yukon Energy Corporation MyAccount Client Portal	Attachment #2
Measures to address vulnerabilities identified in the Security Threat Risk Assessment for the Yukon Energy Corporation MyAccount Client Portal	Attachment #3
Yukon Energy Corporation Retention and Disposition Guidelines RMG-001	Attachment #5
Yukon Energy Corporation Security Procedure RMP-005	Attachment #6
Yukon Energy Corporation and the Yukon Electrical Company Limited Term and Conditions of Service	Yukonenergy.ca

Form Name	Hyperlink or Appendix number
Description of Personal Information Collected (for section 1.1.5 of the PIA)	Attachment #9

1 GENERAL

Department/Corporation:	**Yukon Energy Corporation**
PIA Drafter:	Stephanie Cunha
Program Manager:	Stephanie Cunha

1.1 Project Overview (PIA manual reference: 5.2 Documenting the project)

1.1.1 Description of the Project (PIA manual reference: 5.2.1 Description of the project)

On January 4, 2021, Yukon Energy Corporation (Yukon Energy) will implement an online customer service portal, called MyAccount, to allow its electricity distribution customers to:

- Obtain account information;
- View consumption history;
- Make bill payments; and
- Request changes to the account.

The portal uses the same architecture that is used by the Yukon Electrical Company (doing business as ATCO Electric Yukon) for its Yukon customers.

Yukon Energy customers currently do not have the facility to access account information or pay their bills with credit cards online. An online portal was the most requested service enhancement. Yukon Energy wanted to explore the possibility of offering their customers an on-line service, without having to make a large investment in technology.

In late 2017, Yukon Energy received a demonstration of ATCO Energy's customer portal – MyAccount, which was launched to its customers in 2016. Yukon Energy anticipates the portal will improve customer service and contribute to increased customer satisfaction.

MyAccount is configured as a one-way communication from the existing Yukon Energy Corporation billing system, ATCO CIS, to the new portal, MyAccount.

Customers will be able to launch the portal from the Yukon Energy website or standalone (uniform resource locator) URL.

1.1.2 Scope of PIA (PIA manual reference: 5.2.2 Project scope)

A Yukon Energy customer (user) will register her/his utility account(s) with an email address. Information will be retrieved from Yukon Energy's billing system to ensure that the user requesting access to the account information is in fact the same user in which that electricity account is "owned" by. The Yukon Energy Statement Account Number and Customer Phone Number provided by the customer at the time of registration must match the customer's records in Yukon Energy's billing system.

If the Statement Account Number and Customer Phone Number provided match the records in Yukon Energy's billing system, an email is sent to the user informing him/her of the registration. A link is provided for the user to set a password on the account. Once the user has set the password, he/she can then log into MyAccount.

When a user logs into MyAccount, current information from the customer's billing account is retrieved from the billing system. The customer can view billing history as well as the current bill. The bills will be retrieved on demand through the Bill Presentment (IDS) component of the billing system.

The user will be able to provide updates to his/her account through MyAccount. Changes are emailed (in encrypted format) to Yukon Energy's billing email folder for manual entry into the billing system. The billing email is accessed by less than 10 Yukon Energy customer service and finance team members. If a mailing address is entered, MyAccount uses Canada Post's "Address Complete" functionality to provide a valid mailing address.

A user will also be able to pay their Yukon Energy bill by credit card. MyAccount redirects the user to a Moneris Hosted Pay Page which offers to collect the appropriate credit card information. At no time does Yukon Energy see or store a customer's credit card number.

1.1.3 Parties Involved (PIA manual reference: 5.2.3 Parties involved)

Stakeholder	Function	List Applicable Legislation
Yukon Energy Corporation (Yukon Energy)	Regulated public utility supplying electricity to approximately 2,200 residents and businesses in the Yukon Territory. Yukon Energy policy *CA – 004 Personal Information Privacy Policy for Customers,* Section 5, Purposes, sets out the purposes for the collection of personal information from customers. Specifically, in Section 5.2 in part, Yukon Energy collects your personal information and may use or disclose it for the following reasons: • To provide and administer services requested and to use/disclose information for any purpose related to the operation of your account and the provision of the requested services; • To bill accounts and maintain payment records; and • To provide information to third party service providers, such as account processors and administrators. Section 6 of this policy also covers Consent.	Access to Information and Protection of Privacy (Yukon) s. 29 (c), 35, 36(b) and(c) and Personal Information Protection and Electronic Documents (Canada) s. 5(3) and 6.1
The Yukon Electrical Company Limited (an ATCO company)	Developer of Yukon Energy's billing system and the MyAccount portal. Has a similar customer portal used by some of its customers in the Yukon Territory. The Yukon Energy version of MyAccount will use the same technological platform as the ATCO MyAccount portal.	As a private corporation, it is not subject to Access to Information and Protection of Privacy (Yukon) or Personal Information Protection and Electronic Documents (Canada). The company is subject to the federal Personal Information Protection and Electronic Documents Act (PIPEDA) It is also subject to terms and conditions imposed by contract with Yukon Energy.

Oracle Cloud Platform	The Yukon Energy MyAccount portal is hosted on Oracle Cloud Platform as is ATCO's MyAccount portal	

1.1.4 Objectives and Benefits (PIA manual reference: 5.2.4 Objective and benefits)

By providing a self-service portal to its customers, Yukon Energy anticipates it will improve service and contribute to increased satisfaction.

1.1.5 Description of Personal Information Collected (PIA manual reference: 5.3.1 Types of data (field level or clusters))

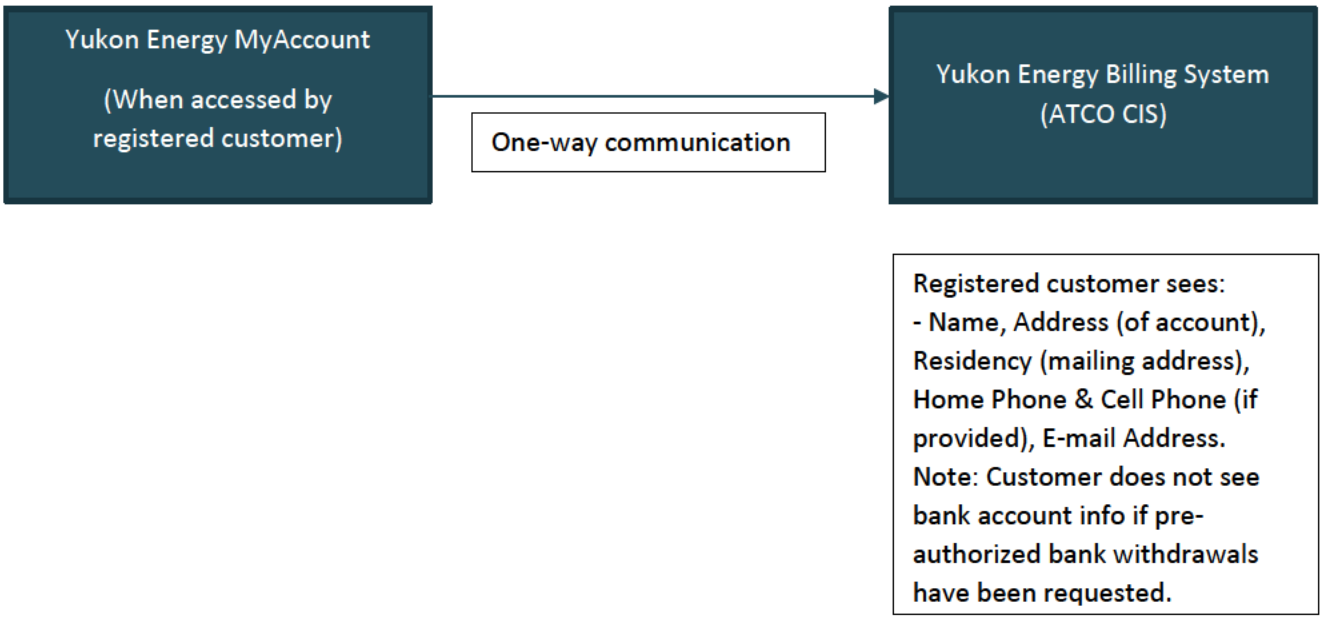
In the excel file below, complete Tab 2: Categories of PI.

See Attachment 9.

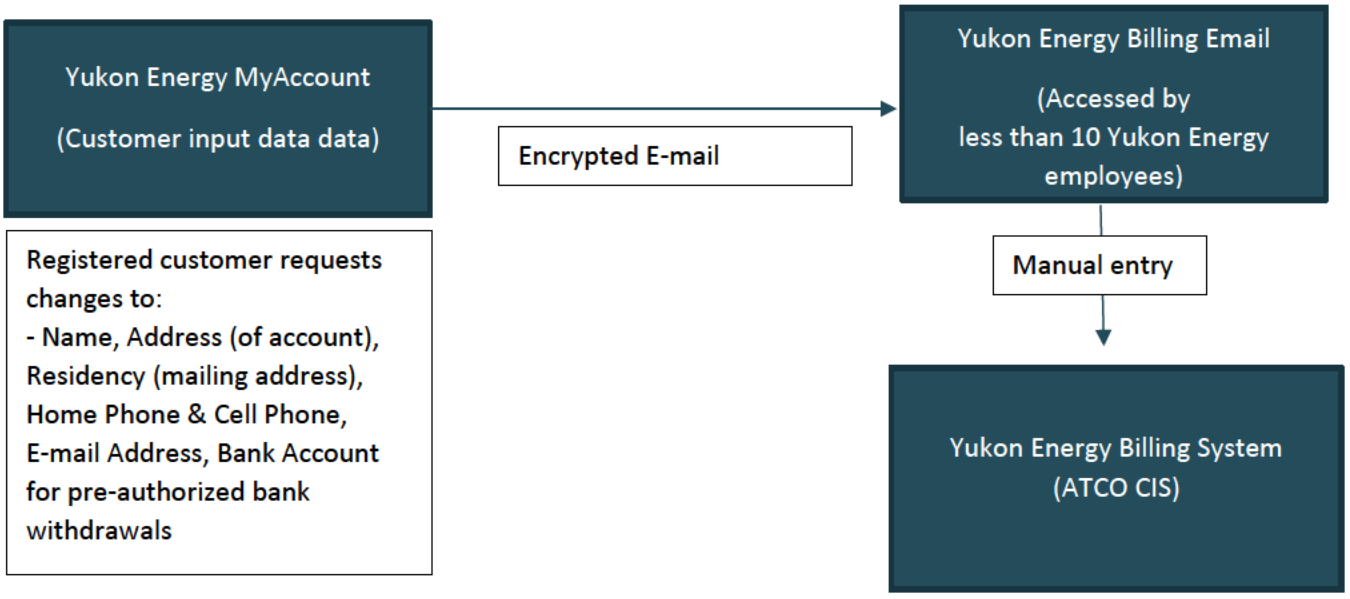
2 Data Flow Mapping and Tables

2.1 Personal Information Flow Diagram and Table (PIA manual reference: 5.3.3 Data flow mapping)

How customer information on MyAccount is obtained for customer viewing:



How data inputted by the customer in MyAccount is updated in Yukon Energy's billing system, ATCO CIS:



NOTE: You need only cite the categories of PI identified when you completed the excel file in question 1.1.6

INFOR-MATION FLOW	DESCRIPTION (Who is it from, who is it going to, who will use it, etc.)	INFORMATION CATEGORY	PURPOSE	LEGAL AUTHORITY (cite specific sections of appropriate legislations)	CUSTODY OR CONTROL (Who is accountable for the information?)
1	Yukon Energy collects Personal Information directly from the Yukon Energy Corporation customer and uses it to provide billing services to the customer's electricity account held with us. Personal Information is collected used and disclosed following consent principle as set out in the company's privacy policy.	Identification and Contact Information	To subscribe to MyAccount	Access to Information and Protection of Privacy Act (ATIPP) Yukon Collection s. 29 (c) Uses. 35(1)(a) and (b)	Custody Yukon Energy Corporation
2	Personal Information is used by Yukon Energy Corporation and disclosed to and used by The Yukon Electrical Company Limited (ATCO) to provide specific services as it relates to the customer's electricity account with Yukon Energy. Yukon Energy Corporation relies on consent as defined in its privacy policy for its collection, use and disclosure of PI to provide service, manage the customer's account and use the MyAccount portal. In event of an emergency, The Yukon Electrical Company (ATCO) can use PI to provide service to Yukon Energy customers. YEC must authorize this use and there are confidentiality provisions in the contract between the two parties.	Identification and Contact Information and Financial Information	The majority of the customer service functions are provided to Yukon Energy Corporation customers by the ATCO Billing System.	Access to Information and Protection of Privacy Act (ATIPP) Yukon Collection s. 29 (c) Uses. 35(1)(a) and (b) And Disclosure s. 36(b) and (c)	Custody Yukon Energy Corporation Control The Yukon Electrical Corporation Limited (ATCO)

3 Privacy Analysis

The following analysis informs the risk summary and mitigation plan of the PIA. Risks identified in the following sections (3.1-3.10) feed directly into the Risk and Mitigation table in section 4.1.

3.1 Accountability (PIA manual reference: 5.5.1 Accountability)

Objective: To ensure a program and public body or custodian designates an individual(s) who is responsible to ensure compliance with privacy legislation. For more detailed information, see section 5.5.1 in the PIA Manual.

Relevant sections of legislation and policy: HIPMA General Regulations s. 16; GAM 2.27 paragraph 3(2)(e) and 3(2)(f).

3.1.1 Identify Information Owner(s)

Name	Position
Stephanie Cunha	Manager, Communications and Customer Service, Yukon Energy

3.1.2 Identify the Department's Privacy Officer(s)

Name	Position
Ed Mollard	Yukon Energy Privacy Officer (also Yukon Energy's Vice President of Finance and Chief Financial Officer)

3.1.3 Identify Third Party Service Providers

For example: Is ICT hosting applications or databases, or are you using a contractor, or both?

Service Provider Name	Services Provided	Written Agreement (Y/N)
The Yukon Electrical Company Limited (ATCO)	Yukon Energy billing system and services to Yukon Energy customers including the development and offering of the My Account portal	Yes

3.1.4 Identify Privacy Risks/Security Threats regarding Accountability

Privacy risks and security threats, including those involving accountability, have been identified and addressed through a security threat risk assessment – see Attachment 2. A list of mitigations completed since the security risk assessment was conducted to mitigate privacy risks and security vulnerabilities is outlined in Attachment 3.

The following table has been intentionally left blank.

#	Privacy Risk/ Threat	Likeli - hood [1]	Impact [2]	Risk Level	Mitigation Strategy	Account- ability	Risk Level After Mitigation

3.2 Identifying Purpose (PIA manual reference: 5.5.2 Identifying Purposes)

Objective: To ensure the purposes for which personal information is collected is identified by the public body or custodian at or before the time the information is collected. For more detailed information, see section 5.5.2 in the PIA Manual.

Relevant sections of legislation and policy: HIPMA Subsection 39(a): the purpose of the collection, use or disclosure of the personal health Information; and subsection 30(2) of the ATIPP Act.

[1] 1. The likelihood of an incident occurring:

HIGH: There is a very good chance that the risk to privacy will occur, particularly if there is a history of it having frequently occurred in this or similar environments.

MEDIUM: There is a good chance that the risk to privacy will occur, particularly if there is a history of it having previously occurred in this or similar environments.

LOW: It is very unlikely that this risk to Privacy will occur.

[2] 2. The impact of the incident should it occur. You should consider the impact on the organization as well as impact on the individuals who are the subject of the personal information:

HIGH: There would be very serious – exceptionally grave consequences if the risk were to occur.

MEDIUM: There would be significant consequences if the risk were to occur.

LOW: There would be low - marginal consequences if the risk were to occur.

Questions for Analysis	Yes	No	N/D or N/A	Details
2.1 What is your legal authority to collect personal information?	Y			Access to Information and Protection of Privacy Act (ATIPP) Yukon Collection s. 29 (c) Uses. 35(1)(a) and (b)
2.2 Is the personal information collected directly related to an operating program or activity?	Y			See Yukon Energy Corporation's and Yukon Electrical Company's Terms and Conditions of Service, approved by the Yukon Utilities Board
2.3 Is personal information being collected directly from the individual or their substitute decision maker? If no, why not?	Y			
2.4 If "no" to 2.3 is the personal information collected from another public body (ATIPP) or a custodian (HIPMA)? Is their disclosure authorized in law?				
2.5 Are positive identifiers collected (e.g. social insurance number, driver's license number, medical record number)? Note in the details if Yukon Health Insurance Plan Number is being collected and indicate whether there is specific authority to collect it.		N		
2.6 Have the purposes for which the personal information is collected been documented? If yes, provide specifics.	Y			The purpose for collection will be explained in the Yukon Energy My Account Client Portal Terms of Uses available at yukonenergy.ca
2.7 Is all the personal information collected necessary to the operating program or activity (put another way, is the program collecting the minimum amount of personal information necessary for the program)?	Y			
2.8 Is there notice at the collection stage that identifies the specific purposes for the collection, the authority for doing so and the individual serving as official contact?	Y			The purpose for collection will be explained in the Yukon Energy My Account Client

				Portal Terms of Uses available at yukonenergy.ca Yukon Energy Corporation's website also has a link to its Customer Privacy Policy and there is instruction on how to contact the company's Privacy Officer
2.9 Is the notice associated with the collection of personal information available and consistent across all mediums of collection?	Y			
2.10 Are secondary uses contemplated for the information collected? If yes, describe them in the details column.		N		
2.11 If personal information is to be used or disclosed for a secondary purpose not previously identified, is consent required?			N/A	
2.12 If consent is not required for secondary purpose use or disclosure, is there authority for the use or disclosure?			N/A	
2.13 Is personal information collected from a public database?		N		
2.14 Will program evaluation, quality assurance or security activities result in the collection of additional personal information?		N		
2.15 Does the program or activity involve the collection through a common client identifier? If yes, provide details about the identifier.	Y			Statement account number for the customer is common with that in Yukon Energy's billing system.

3.2.1 Describe how your project has notified the individual the purpose for which the personal information is being collected? Include sample collection notice.

See link to Yukon Energy's Customer Privacy Policy
https://yukonenergy.ca/customer-service/accounts-billing/customer-personal-information-and-privacy/customer-privacy-policy

Also link to Yukon Energy's "Terms of Use" for the MyAccount client portal
https://yukonenergy.ca/customer-service/accounts-billing/my-account-client-portal-terms-of-use

3.2.2 Identify Privacy Risks/Security Threats regarding Identifying Purpose

Risk	Description
2-1	*Yukon Energy customers are choosing to use the portal service and the project is collecting minimal additional personal information (e.g. email address), therefore no new risks regarding identifying purpose have been identified.*

3.3 Consent (PIA manual reference: 5.5.3 Consent)

3.3.1 Is consent being utilized as an authority to collect, use and/or disclose personal information?

Consent is being used as the authority to collect, use and disclose personal information. Yukon Energy's Customer Privacy Policy developed in compliance with the federal Personal Information Protection and Electronic Documents Act, sets out when consent is required for collection, use and disclosure and those situations when consent is not required.

The policy covers the purposes for which the personal information is collected, used or disclosed and limitations on those actions. The policy also covers how access is provided and where complaints and questions can be directed. Further, the policy covers safeguarding and accuracy of the personal information.

The policy also addresses sections of the Access to Information and Protection of Privacy Act by addressing that personal information will be collected directly from the individual with consent as per s. 30(1)(a)(i) and (c) (iii) and sets out the legal authority for collection as per s. 30(2). The policy also covers accuracy of personal information (s. 31), the process to make correction to personal information (s. 32),

how personal information is protected (s. 33), the use of the personal information (s. 35) and why it is disclosed (s. 36).

The policy covers how an individual may withdraw consent.

The policy covers how consent may be given and whether consent is required or not.

3.3.2 Identify Privacy Risks/Security Threats regarding Consent

Risk	Description
3-1	*Yukon Energy customers are choosing to use the portal service and the project is collecting minimal additional personal information (e.g. email address) therefore no new risks regarding consent have been identified.*

3.4 Collection of Personal Information (PIA manual reference: 5.5.4 Limiting collection)

The legal authority to collect the personal information is from the Yukon Territory's Access to Information and Protection of Privacy (Yukon) s. 29 and from the federal Personal Information Protection and Electronic Documents (Canada) s. 5(3).

The personal information will not be used for secondary purposes; it will only be used to update the customer's existing electricity account with Yukon Energy and information displayed on the MyAccount portal.

For the Yukon Energy customer who chooses to use this service (the reasonable person), the collection is limited to that which the reasonable person would consider as necessary to provide the service.

A customer's Statement Account Number and Phone Number are used to identify the customer at the time that someone looks to register with MyAccount. The Statement Account Number and the Customer Phone Number must match Yukon Energy's billing records for that account. This data matching would be considered reasonable and consistent with the stated purpose of the MyAccount portal by the Yukon Energy customer.

Reports of usage by and the number of subscribers to the portal are aggregated.

3.4.1 Describe how personal information is collected directly from individuals.

At minimum, address the following in your response:

- *Whether it was collected directly from*
  - *The individual?*
  - *An authorized representative (include sample of authorization)?*
  - *Parent or guardian?*
- *Whether it was collected via*
  - *Electronic form?*
  - *Paper form?*
  - *Faxed to the program?*
  - *Emailed to the program?*

Yukon Energy customers will choose to use the MyAccount portal and the customer will directly provide his/her information by inputting the required information into the portal.

3.4.2 Describe how personal information is collected indirectly from individuals.

Note: Review relevant policies and legislation to ensure compliance: HIPMA Section 54: Where Indirect Collection is permitted; HIPMA: Collection of Personal Health Information Policy; ATIPP Section 30: How Personal Information is to be Collected; ATIPP: Collection of Personal Information Policy.

Not applicable

3.4.3 Has the program conducted a review of the personal information collected to ensure only the minimum necessary is being collected?

Yes, the review was conducted by Stephanie Cunha and Ed Mollard of Yukon Energy in December 2020.

3.4.4 Identify Privacy Risks/Security Threats regarding Collection

Yukon Energy's MyAccount portal uses infrastructure for storage of customer personal information that is of a similar configuration to that used by Yukon Electric Company Limited (ATCO) and other ATCO North of 60 companies. It is a tested infrastructure. It is hosted on Oracle Cloud infrastructure, which is a known and tested cloud service.

Data at rest is contained in Oracle databases which are encrypted data centre with offsite disaster recovery site backup copy on encrypted storage. Most sensitive data are transient and only reside in the system for the duration of the user session. Session timeout is 30 minutes.

Risk	Description
4-1	*To utilize tested infrastructure, Yukon Energy has to use third parties (ATCO and Oracle) for the MyAccount portal project. Yukon Energy has agreements in place with ATCO that cover data confidentiality and required security and data separation provisions. ATCO has agreements with Oracle that cover data confidentiality and required security and data separation provisions.*

3.5 Use, Disclosure and Retention of Personal Information (PIA manual reference: 5.5.5 Limiting use, disclosure, and retention)

Objectives:

(1) To ensure personal information is used and disclosed for purposes it was collected, except with the consent of the individual or if authorized by law.

(2) To ensure personal information is retained only as long as necessary for the fulfillment of the stated purposes and is destroyed as authorized by law. For more information, see section 5.5.5 of the PIA Manual.

ATIPP Section 35: Use of Personal Information; ATIPP Sections 36 – 39: Disclosure of Personal Information; ATIPP Policies: Use and Disclosure of Personal Information; Archives Act Records Management Regulations Section 5.

The MyAccount portal initiative will not use information already collected by Yukon Energy to deliver and bill customers for electricity for any new purpose; the portal is simply a more convenient way for a Yukon Energy customer to access their own billing, account and consumption information already held in the billing system and delivered monthly to them on their power bill.

Yukon Energy customer data is already stored in Yukon Energy's billing system, ATCO CIS. Yukon Energy customer information is disclosed to ATCO as ATCO is the supplier and service provider for Yukon Energy's billing system. The implementation of the MyAccount client portal does not change or impact this arrangement. Information is transferred in encrypted format through a virtual private network (VPN).

The authority to disclose the personal information is from the Access to Information and Protection of Privacy Act s. 36(b) and (c). The personal information is disclosed with the consent of the individual.

A Yukon Energy customer's unique Statement Account Number and Customer Phone Number are used as primary identifiers to confirm the customer's identity before access to MyAccount is granted. Once initial access is granted, the customer's unique email address and password must be used to access the MyAccount site.

The Oracle Cloud platform that is used for MyAccount portal uses an off-site backup data centre located in the United States. Only the customer's user id and related statement account number is stored there. No personal information, customer account or billing data is retained on site.

Yukon Energy customer data is not disclosed to another public body or custodian.

Encrypted emails issued by the MyAccount system to Yukon Energy customer service staff outlining customer requests made on the MyAccount system will be retained for seven years. These files will be securely disposed of according to Yukon Energy's records management policies and procedures. See Attachments # 4, 5 and 6.

3.5.1 Does your project use personal information to make decisions that directly affect(s) an individual(s)?

For example: A determination about whether an individual is entitled to income assistance, a decision on hiring an individual, or a determination about eligibility for subsidized housing.

At minimum, address the following in your response:

- *Describe what measures will be taken to ensure personal information will be retained for at least one year.*

The personal information collected will not be used to make decisions that affect the individual. Encrypted emails issued by the MyAccount system to Yukon Energy customer service staff outlining customer requests made on the MyAccount system will be retained for seven years.

3.5.2 What secondary uses or disclosures are contemplated for the personal information collected?

At minimum, address the following in your response:

- *What the information will be used or disclosed for;*
- *What organization will the information be used by or disclosed to;*
- *Whether consideration has been given to de-identifying the information;*
- *Whether data-linking will occur;*
- *Whether unique identifiers will be used or assigned;*
- *Whether a formal agreement has been entered into.*
    - *Does the agreement adhere to policy requirements? For example, as defined in the "Agreements" section in the Disclosure Personal Information Policy for ATIPP.*

Secondary uses of Yukon Energy customer data are not contemplated by this project.

Yukon Energy customer data is already stored in Yukon Energy's billing system. Yukon Energy customer information is disclosed to ATCO as ATCO is the supplier and service provider for Yukon Energy's billing system. The implementation of the MyAccount client portal does not change or impact this arrangement. There is a contractual agreement in place between to Yukon Electrical Corporation Limited (ATCO) and Yukon Energy that outlines these services and includes confidentiality clauses.

3.5.3 Describe how personal information is used for evaluation or planning purposes.

Not applicable

3.5.4 Does the project disclose personal information for research or statistical purposes? If yes, please explain and attach the research agreement.

Not applicable

3.5.5 Has a Records Retention and Disposition Schedule been completed?

Note: Refer to your Information/Records Officer if you do not have access to a Records retention and Disposition schedule. Refer to Archives Act Records Management Regulations Section 5 for more information.

Please see Attachment # 4 for Yukon Energy's Record Management Policy and Attachments # 5 and 6 for two of Yukon Energy's records management procedures as they relate to disposing of records and security.

3.5.6 Identify Privacy Risks/Security Threats regarding Use, Disclosure, Retention Disclosure

Risk	Description
5-1	A security threat risk assessment (STRA) has been completed for the project which is provided as an attachment # 2 and # 3 to the privacy impact assessment.

3.6 Accuracy of Personal Information (PIA manual reference: 5.5.6 Accuracy)

Objective: To ensure personal information is accurate, complete and up-to-date for the required purpose. For more information, see section 5.5.6 of the PIA Manual

Relevant sections of legislation and policy: HIPMA Section 52: Accuracy of Information Collected; HIPMA Section 28: Correction of Personal Information; ATIPP Section 31: Accuracy of Personal Information; ATIPP Section 32: Right to Request Correction of Personal Information.

3.6.1 Describe the steps taken to ensure that the personal information is accurate, complete and up-to-date.

For example: records indicate the date the information was last updated; the information systems logs corrections or modifications to information

The Yukon Energy customer (user) is entering his/her information into the MyAccount portal. There is minimal data entry required to set up user access to the portal and to display information, therefore the possibility of errors in data entry and the need for correction are minimized.

The user will be able to provide updates to his/her account through MyAccount. Changes are emailed (in encrypted format) to staff in Yukon Energy for manual entry into the Yukon Energy billing system. If a mailing address is entered, MyAccount uses Canada Post's "Address Complete" functionality to provide a valid mailing address.

3.6.2 Describe how an individual's information will be updated or corrected.

The user will be able to provide updates to his/her account through MyAccount. Changes are emailed to staff in Yukon Energy for manual entry into the Yukon Energy billing system. If a mailing address is entered, MyAccount uses Canada Post's "Address Complete" functionality to provide a valid mailing address.

3.6.3 Identify Privacy Risks/Security Threats regarding Accuracy

Risk	Description
6-1	The MyAccount portal project introduces very minimal new privacy risk or security threats related to data accuracy.

3.7 Safeguarding Personal Information (PIA manual reference: 5.5.7 Safeguards)

Objective: To ensure personal information is protected against unauthorized access, collection, use, disclosure, retention and disposal. For more detailed information on safeguarding personal information, see section 5.5.7 in the PIA Manual and Schedule 3: Detailed Technical and Security Questionnaire in the PIA Manual.

Relevant sections of legislation and policy: HIPMA Section 19: Custodian's Information Practices Generally and HIPMA General Regulation Section 14: Custodian's Information Practices; ATIPP Section 33: Protection of Personal Information

3.7.1 Has a Security Threat Risk Assessment (STRA) been completed?

A security threat risk assessment has been completed and is provided as Attachment 2 to the privacy impact assessment. Attachment 3 outlines the mitigations that Yukon Energy has put in place to address the vulnerabilities identified in the assessment.

3.7.2 Describe how users are authenticated before accessing the information.

Objective: To corroborate that a person is the one claimed.

At minimum, address the following in your response:

- *What method is used:*
  - *Something the individual knows; a password or PIN, for example.*
    - *Are passwords known only to the authorized user of the account?*
    - *Where authentication is based on username and password, are effective password policies in place and do they adhere to YG's corporate password policy?*
  - *Something the individual has; a swipe card or token, for example.*
  - *Something the individual is; a fingerprint, voice scan or retinal scan, for example.*
- *Are users assigned a unique name and/or number for identifying and tracking user identity?*
- *What is the current format used for unique identification?*
- *Can the unique user identifier be used to track user activity within the information system?*
- *Does the information system have automatic logoff capability whereby users must re-authenticate to access the information system?*

In the Security Threat Risk Assessment (STRA) for the project – see End Users and Administrators, pages 12 and 13.

To register with MyAccount, a Yukon Energy customer must visit yukonenergy.ca or the MyAccount url.

As part of the registration process, the customer must provide an email address, their Yukon Energy Statement Account Number and the Customer Phone Number that is on the customer's account.

Information will be retrieved from Yukon Energy's billing system to ensure that the user requesting access to the account information is in fact the same user in which that electricity account is "owned" by. The Statement Account Number and Customer Phone Number provided by the customer at the time of registration must match the customer's records in Yukon Energy's billing system.

If the Statement Account Number and Customer Phone Number provided match the records in Yukon Energy's billing system, an email is sent to the customer informing them of their registration. A link is provided in that email for the customer to set up a password. Once the user has set the password, they can then log into MyAccount using their email address and their password.

Passwords must be at least 8 characters, have two of four character types and no same three characters in a row. The account is locked after five failed attempts. Password, as well as all other data, is encrypted at rest and in transit.

When a user logs into MyAccount, current information is retrieved from Yukon Energy's billing system. The customer can view billing history as well as the current bill. The bills will be retrieved on demand through the Bill Presentment (IDS) component of Yukon Energy's billing system. There is a 30 minute inactivity time out of the user session.

The user will be able to provide updates to his/her account through MyAccount. Changes are emailed to staff in Yukon Energy for manual entry into ATCO CIS. If a mailing address is entered, MyAccount uses Canada Post's "Address Complete" functionality to provide a valid mailing address.

3.7.3 Describe how access to the information is controlled.

Objective: Only individuals with a need to know have access to data; based upon job duties, restrict user functions to view, read, write, delete, and/or execute roles.

At minimum, address the following in your response:

- *Are access privileges limited to the least amount of personal information required to carry out job-related functions?*
- *What method(s) is/are used?*
  - *User-based access: An individual has access to data based on who he or she is.*
  - *Role-based access: An individual has access to data based on his or her role within the organisation.*
  - *Context-based access: An individual has access to data based on where and when he or she is accessing the data. Context-based access also incorporates user-based and/or role-based access to authenticate the user.*
- *Is there an access control policy?*
  - *Does the access control policy clearly state the information access privileges for each defined role in the information system?*
  - *Does the access control policy clearly state the information access privileges for each defined role in the information system?*
  - *Is a formal user registration process in place?*

        - *Does the user registration process include: verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not granted until formally approved?*
        - *Is a current, accurate inventory of computer accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts?*
    - *Is there a formal process to assign defined roles to users?*
    - *Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals?*
- *Are users given a written statement of their access rights and required to sign that they understand the conditions of access?*

See Access section of STRA page 14.

A Statement Account Number and Customer Phone Number provided by the Yukon Energy customer at the time of registration must match the customer's records in Yukon Energy's billing system.

If the Statement Account Number and Customer Phone Number provided match the records in Yukon Energy's billing system, an email is sent to the customer informing them of their registration. A link is provided in that email for the customer to set up a password. Once the user has set the password, they can then log into MyAccount using their email address and their password.

See Administrators section of STRA page 13. An Administrator requires an Active Directory account and multi factor authentication to gain access.

3.7.4 Describe how you will audit or track who accessed information.

Application and system logs are in place with alerting (see pages 15 and 16 of the STRA Attachment # 2) and are now being monitored (see Attachment # 3) by ATCO Group.

3.7.5 Describe where and how information is transmitted.

Objective: To safeguard against unauthorized access and modification during transmission (both physical and electronic information).

At minimum, address the following in your response:

- *How does your program transmit information?*
    - *How often does your program transmit information?*
    - *Is there a procedure in place to ensure that any removal of personal information from the premises has been properly authorized?*
- *Is data encrypted to prevent access by individuals without access rights?*
    - *Encryption is recommended for the following:*
        - *Back-up media that must leave the facility*
        - *Emails containing sensitive information*
        - *Laptops or mobile devices containing sensitive information*
        - *Internet sessions involving sensitive information*
        - *Any remote access sessions involving sensitive information*
    - *What method of encryption will be used?*

For data transmission, see Integrated Systems section of STRA page 13.

For encryption, see Application section of STRA page 13 and Operating Systems section of STRA page 16.

3.7.6 Describe where and how information is stored.

Objective: To safeguard against unauthorized access and modification at rest (both physical and electronic information).

At minimum, address the following in your response:

- *Where is information stored?*
  - *Is i*nformation is stored in a SQL database on a server in the ICT data centre; on a third party's server; filing cabinets?
- *Is data encrypted to prevent access by individuals without access rights?*
  - *What method of encryption will be used?*

See Data location section of STRA page 12.

The data is stored in the Oracle Cloud Platform. The production data centre is located in Canada and the disaster recovery site in the United States. https://docs.cloud.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm

3.7.7 Describe the physical security measures taken to protect the personal information.

Yukon Energy Corporation's Security Procedure RMP 005 applies to customer data collected by the MyAccount initiative. See Attachment # 6.

3.7.8 Describe the technical security measures taken to protect the personal information.

Objective: To secure the information system and the networks on which the data and information reside.

At minimum, address the following in your response:

- *Does the organization use a variety of mechanisms (e.g. firewalls, routers, intrusion detection and prevention systems, audit logs, system performance tools, etc.) to continuously monitor the operations of their systems to detect anomalies in service delivery levels?*
  - *Are systems that are exposed to a public network "hardened"?*
  - *Does the LAN that is connected to a public network use perimeter defence safeguards?*
  - *If wireless devices are used, are the strongest security features of the wireless device enabled (encrypted and authentication, for example)?*
  - *Is a wireless intrusion detection system employed?*
- *Are operating systems kept up-to-date with patches and fixes?*
- *Is there a regular schedule for updating definitions and running scans with anti-virus, anti-spyware and anti-rootkit software?*
- *Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?*
- *Are all system/audit logs that relate to the handling of personal information regularly monitored?*
- *Are procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly?*
- *Are backup processes in place to protect essential business information such as production servers, critical network components, configuration backup, etc?*
- *Are there controls that prevent or detect unauthorized software?*
- *Is there a patch management process for new security vulnerabilities?*

Technical security measures are drawn from the Oracle Cloud environment.

See Data Location and Backup and Retention Capabilities of STRA page 12.

See Administrators and Authentication Type of STRA page 13.

See Compliance – Hosted Infrastructure and Data Processing – Data Validation of STRA page 14.

See Infrastructure – Network of STRA pages 15 and 16.

See Infrastructure – High availability capabilities of STRA page 16.

See Operating Systems – Security context and Monitoring of STRA page 16.

See Security Program section of STRA page 17.

The Oracle Cloud environment includes firewalls, intrusion detection and prevention measures, access and event audit logging and system performance monitoring for denial of service attacks and other threats.

ATCO has deployed System Event and Information Management (SIEM) software to assist with analysis of logging and provides notification of significant events. The reports from the SIEM system are regularly monitored by ATCO Group.

MyAccount is a public facing portal and therefore the number of TCP (Transmission Control Protocol) ports that are open has been reduced to the minimum required to permit the required functionality for public access. See Attachment #2 STRA pages 15 and 21, and Attachment # 3.

Wireless networks are not used for the MyAccount portal. Customers are able to use wireless networks to connect to MyAccount.

Both Oracle Cloud and Yukon Energy's billing system do regular updates to operating systems, firewalls and software used to detect malware. Both Oracle Cloud and Yukon Energy's billing system have authorization processes for upgrades and have the ability to detect changes to software. There are scans done for reports of new security vulnerabilities and patches are applied as required and/or other mitigation measures are taken.

There are disaster recovery processes and backup and restore processes for both the Oracle Cloud and the Yukon Energy's billing system that are tested on an annual basis. Backup includes application data, operating system and application programming. The Oracle Cloud infrastructure is designed as high availability with redundancies for networks and servers. See Attachment # 2 STRA page 12 and Attachment # 3.

3.7.9 Describe the administrative security measures taken to protect the personal information.

Objective: To control human behaviour through clearly written policies and procedures.

All Yukon Energy employees must read and sign off the Corporation's Records Management Policy at the time of hire – see Attachment 4. Section 5 of the policy relates to Privacy. It outlines all employees' responsibilities to ensure that appropriate security measures are observed for confidential information. The policy also outlines confidentiality and security of information as a condition of employment.

Yukon Energy also has an ATIPP policy – see Attachment 7.

There is a contractual agreement in place between to Yukon Electrical Corporation Limited (ATCO) and Yukon Energy that outlines confidentiality clauses of information stored in Yukon Energy's billing system.

3.7.10 Identify Privacy Risks/Security Threats regarding Safeguards

Risk	Description
7-1	*For Attachment # 2 (STRA) see Table 5 beginning on page 18 and continuing to page 21 and Table 8 on page 23.*

MakeIT completed a third-party Security Threat Risk Assessment of the MyAccount portal in August 2020. Five risks were identified (see page 18 – 21 of Attachment # 2). Since that time, Yukon Energy has worked with ATCO to mitigate each of the five risks. Actions taken are outlined in Attachment # 3

As a result of these actions, Yukon Energy is confident that all security threats have been appropriately mitigated.

3.8 Openness (PIA manual reference: 5.5.8 Openness)

3.8.1 Describe how policies and procedures related to the management of personal information are made available to the public.

Yukon Energy's website has a link to its Customer Privacy Policy and there is instruction on how to contact the company's Privacy Officer – please use the link below

https://yukonenergy.ca/customer-service/accounts-billing/customer-personal-information-and-privacy#:~:text=Yukon%20Energy%20is%20committed%20to%20respecting%20the%20privacy%20of%20your%20personal%20information.&text=Personal%20information%20is%20kept%20only,arrangements%20to%20protect%20the%20information.

Also see Terms of Use for the MyAccount Portal

https://yukonenergy.ca/customer-service/accounts-billing/my-account-client-portal-terms-of-use

3.8.2 Identify Privacy Risks/Security Threats regarding Openness

Risk	Description
8-1	Customers of Yukon Energy are choosing to use the portal service and the project is collecting minimal additional personal information (e.g. email address) therefore no new risks regarding openness have been identified.

3.9 Individual Access to Personal Information (PIA manual reference: 5.5.9 Individual access)

3.9.1 Describe how access to the personal information will be facilitated.

Please see "Providing Access" section of the Yukon Energy' privacy policy

https://yukonenergy.ca/customer-service/accounts-billing/customer-personal-information-and-privacy/customer-privacy-policy

3.9.2 Has a Personal Information Map been completed for this project?

Note: Complete Tab 3: PI Map (Inventory) from the excel file you completed when answering question 1.1.6.

3.9.3 Identify Privacy Risks/Security Threats regarding Access/Correction

Risk	Description
9-1	Customers of Yukon Energy Corporation are choosing to use the portal service and the project is collecting minimal additional personal information (e.g. email address) therefore no new risks regarding correction have been identified.

3.10 Challenging Compliance (PIA manual reference: 5.5.10 Challenging compliance)

Yukon Energy's Privacy Policy does provide measures to challenge compliance.

https://yukonenergy.ca/customer-service/accounts-billing/customer-personal-information-and-privacy/customer-privacy-policy

3.10.1 Are policies and procedures related to the management of personal information available to the public?

Yes please see link in response to question 3.8.1.