Privacy Impact Assessment (PIA) for

Eddie software for Level 3 charging Station

Before you start 1

PART 1: GENERAL INFORMATION 2

PART 2: COLLECTION, USE, AND DISCLOSURE 6

PART 3: STORING PERSONAL INFORMATION 8

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 9

PART 5: SECURITY OF PERSONAL INFORMATION 12

PART 6: ACCURACY, CORRECTION AND RETENTION 14

PART 7: PERSONAL INFORMATION BANKS 16

PART 8: ADDITIONAL RISKS 16

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act.* FIPPA's protection of privacy requirements. A PIA is a legislative requirement (FIPPA s. 69(5.3)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.
- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.

- Please review the initial assessment questions and contact the Privacy Office at privacyandfoi@vcc.ca before you begin the form, if you have not already. See more guidance about the PIA process, including the supplementary Guidance Document, on the <Privacy web site>.

PART 1: GENERAL INFORMATION

PIA file number: #2024-012

Initiative title:	Eddie software for Level 3 charging Station
VCC Department / Program Area:	Heavy Duty Mechanic
Link to VCC initiative website:	n/a
Link to vendor website:	Charger: chargefwd.com Eddie: www.axso.co
Link to vendor privacy policy:	https://fr.axso.co/terms-and-conditions https://eddie-prod-documents.s3.ca-central-1.amazonaws.com/privacy-policy-en.pdf
Your name and title:	Feras Ghesen: Associate Director, School of Trades, Technology and Design
Your work phone and email:	778-879-4138 email: fghesen@vcc.ca
Initiative Lead name and title:	Brett Griffiths, Dean, School of Trades, Technology and Design Paul Cory, Department Head for HMT
Initiative Lead phone and email:	604-488-4204 bgriffiths@vcc.ca pcory@vcc.ca 778-788-6931

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	NO
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy	NO

Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	
Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an Information Sharing Agreement.	NO
Related PIAs, if any:	

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved, and when or how long your initiative runs. If this is a change to an existing initiative, please also explain the change and the benefits of the change.

Eddie is an electric vehicle energy management system that is designed for multi-dwelling units, created by AXSO/Hydro-Quebec. The system offers a number of features for monitoring electric vehicle charging, payment, and locating charging stations. Chargefwd is the reseller for both the charger and the software for VCC.

At VCC, the Edde software is being used in a very limited scope and only to manage the Level 3 Charger/Charging Station in the Heavy Mechanic Shop, s. 15(1)(l) . The software will:

- s. 15(1)(l)
  - Not be assigned to any individual (only one purpose-specific account will be created); and
  - Be used only for the purpose of running this software and managing the Charger.
- Only be used by VCC employees (no students). Only Heavy Mechanic Trades staff will have access to the software and its charging logs;
- Only collect information on the use of the Level 3 Charger, including length of charging, kWh delivered, and time of the day.

VCC will not pay through the app because this software is only being used to manage and track the vehicle charging sessions. The initiative will be ongoing as the software will be used to manage the Charger for the foreseeable future.

2. What is the scope of the PIA?

Your initiative might be part of a larger initiative or might be rolled out in phases. What part of the initiative is covered by this PIA? (An initiative may require multiple PIAs.) What is out of scope of this PIA?

The scope only involves the use of the Eddie software for one purpose-specific VCC account on one dedicated VCC device for one charger, the Level 3 Charger. If the software is added to any individuals' mobile devices in the future or the creation of individual accounts is required, especially if the account creation involves students, this PIA should be revised.

3. What are the data or information elements involved in your initiative?

*Please list **all** the elements of information or data that you might **collect, use, disclose, store, or access** as part of your initiative (**including but not limited to personal information**). Please:*

- *include where the information is coming from (e.g. collected directly from users, pulled from existing databases, etc.);*
- *group different categories of people together (e.g. students, employees, alumni, etc.) if your initiative involves large quantities of information or datasets.*

Eddie has the capability to collect information through registration and use of the software, both for its intended use and information on the user. Potential data collection includes:

Account Registration:

- Email address
- First and Last Name
- Contact information: telephone number, postal address
- Geolocation with user's consent (optional)
- Profile photo (optional)
- Payment information (only credit card imprint; software does not collect credit card information)

Logs of Charging Sessions: Information about the charging sessions (length, kWh delivered, members who access the Charger, time of the day)

Collection by App/Software:

- Information relating to use of Eddie: user ID, password, activities when the user is connected to the platform and recharging activity
- Model, make, and version of device or Web browser and its unique identifier
- Any personal information that may be provided to Eddie/AXSO during interactions.

VCC will create an email address and account for the Charger that will not be associated with an individual for the purpose of using this software, and VCC will only use the Eddie software on a dedicated mobile device that will also not be associated with an individual. This way, VCC will ensure that no personal information is collected through registration or through the use of the software/device. VCC will not be paying through the Eddie software and will turn the geolocation option off.

In VCC's use of Eddie, collection will include:

- Email address s. 15(1)(l)
- VCC address and contact information (not associated with an individual)

- Logs about the charging session (no information about members will be collected, due to there only being one general Charger account and the mobile device remaining located with the Charger)
- Information collected by the software – but none will be related to an identifiable user because of the Charger account and the mobile device remaining on site.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference. This includes, but is not limited to:

- *Names, home addresses, emails, and telephone numbers of the individual or their guardians and family members (this includes student names and emails!);*
- *Images of an individual;*
- *Identifying number (e.g. student number, employee number, health care number);*
- *An individual's personal views or opinions, or anyone else's opinions about an individual;*
- *Educational, medical, medical, criminal, financial, or employment history.*

No – Eddie has the ability and the potential to collect personal information, as listed in #3, but VCC is taking steps to ensure that no personal information is collected through the design of this initiative, as detailed throughout this PIA.

- If no, answer question 4.
- If yes, are all of the personal information elements **necessary** for your initiative?
    - [Answer: Yes or No], then skip question 4 and continue to Part 2

4. If you answered "no" to question 3.1: How will VCC reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in a privacy breach or other privacy incident. After you answer this question, submit this PIA to the Privacy Office. You do not need to complete the rest of the PIA template.

- VCC will create a general account for use with the Eddie software, using a purpose-specific VCC email address and no personal information. s. 15(1)(l)
- The general account will use a VCC email address created for this purpose and will not use any individual's personal information in the creation of the account.

- VCC staff will be advised not to create any new accounts.
- If VCC finds that new accounts are needed to use with new chargers, they should also be created using purpose-specific emails/accounts that do not collect any personal information.
- VCC will turn off the geolocation option and disable other analytics options.

Although the initiative is not collecting personal information, Part 5 and Part 8 of this PIA are completed to acknowledge the risk of collection of PI.

PART 2: COLLECTION, USE, AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use, and disclosure flow

Describe the information flow of your initiative in the chart below. The table explains the movement of personal information throughout your initiative (column 1) and identifies each time personal information is collected, used, or disclosed (column 2) and under which corresponding FIPPA authority (column 3).

- ***Collection:*** *Describe the steps in collecting personal information from individuals by VCC and/or the vendor (clarify which party is collecting the information).*

- ***Use:*** *How does VCC and/or the vendor use personal information (clarify which party is using the information)?*

- ***Disclosure****: When, if ever, would VCC and/or the vendor provide the personal information to an internal or external third party that does not normally have access to the personal information?*

Use column 4 if there are any specific potential risks related to each step. Change the information flow and add more rows as necessary. The red text below is an example – input the steps and relevant authorities to reflect your initiative's flow.

For the most common FIPPA authority references to assist with completing this chart, please see Section 1 of the Guidance Document, or consult the full text of Part 3 of FIPPA.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority or other legal authority	Specify any potential risks

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice and Consent

6. 1 Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA s. 27(2) requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of VCC, the vendor must also provide a collection notice. FIPPA requires that you notify the individual of:

- *the legal authority,*
- *purpose(s) and use of their personal information (including any third party disclosures), and*
- *contact information or someone who can answer questions about the collection and use.*

Review the template collection notice below and update as applicable.

Collection notice template (complete or replace with your notice):

Your personal information is collected under the authority of [applicable authority from FIPPA s. 26] of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA) [and/or any other federal or provincial laws that provide specific legal authority if applicable]. This information will be used for [program/activity/other purpose for collecting the information]. Questions about the collection of this information may be directed to [title and business email of the role who can answer questions, ideally from relevant program area].

The collection notice will be posted [location].

Not applicable

6. 2 Consent

If you are obtaining consent for the use or disclosure of personal information (indicated by the FIPPA authorities you used in Question 5), add any consent language here.

Consent must have the following elements:

a) be in writing; and
b) be done in a manner that specifies:
    a. the personal information for which the individual is providing consent;
    b. the date on which the consent is effective and, if applicable, the date on which the consent expires;
    c. for "use" consent, the use of the personal information; and
    d. For "disclosure" consent:
        i. to whom the personal information may be disclosed;
        ii. if practicable, the jurisdiction to which the personal information may be disclosed; and
        iii. the purpose of the disclosure of the personal information.

[Answer only if required – Provide your consent language] Not Applicable as we don't collect any personal information.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

[Answer: Yes or No]

- If no, skip to Part 5.

8. If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?

Be specific about the location where the personal information is stored (e.g. which state(s) or country/countries).

[Answer]

9. Does your initiative involve sensitive personal information that will be stored outside of Canada?

Sensitive personal information is not defined in FIPPA. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored. Common sensitive personal information could include: personal health or medical information; financial information; criminal records; disciplinary or complaint history; unique government issued identifiers (passport number, driver's license, personal health number, SIN); racial or ethnic origins; sexual orientation; religious or philosophical beliefs; etc. Please see the above link for more guidance or consult with VCC's Privacy Office.

[Answer: No]

- If yes, go to question 10
- If no, skip ahead to Part 5

10. If you answered "yes" to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?

[Answer: Yes or No]

- If yes, what enactment?
  - [Answer] then skip ahead to Part 5.
- If no, go to Part 4.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section **only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada**. This section will require consultation with a representative from IT Services.

11. Is the sensitive personal information stored by a service provider?

[Answer: Yes or No]

- If yes, fill in the table below (add more rows if necessary) and then go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. If you answered "no" to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

This should include reference to the location and method of storing the personal information (e.g. location of data: Atlanta, GA, USA. Method of storing data in Atlanta, GA, USA: e.g. specify that the information is stored in a data storage facility).

[Answer]

13. Does the contract you rely on include privacy-related terms?

[Answer: Yes or No]

- If yes, describe the contractual measures related to your initiative.
    - [Answer]
- Is VCC's Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative's contract? [Answer: Yes or No]

14. What controls are in place to prevent unauthorized access to sensitive personal information?

Describe technical, security, administrative and/or policy measures that are in place to protect against the unauthorized collection, use, disclosure or storage of sensitive personal information, including preventing or managing access to sensitive personal information. If your initiative uses a cloud-based service provider, also consider controls at each layer: software, platform, and infrastructure.

See Section 2 of the Guidance Document for examples of these measures and consult with IT Services to answer this question.

[Answer]

15. Provide details about how you and will track access to sensitive personal information.

Describe how you will know if the sensitive personal information is accessed, including access by service providers (e.g. logging access to data). Consult with IT Services to answer this question.

[Answer]

16. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence, and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary. See Section 3 of the Guidance Document for examples of privacy risks and risk responses and more guidance for how to complete this table, or see the Guidance on Disclosures Outside of Canada.

Privacy risk	Impact to individuals (low, medium, high)	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the role designated accountable for the initiative on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 16.

Is the outcome to proceed with the initiative? [Answer: Yes or No]

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5, you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

***This section completed due to the potential to collect personal information.**

17. Does your initiative involve digital tools, databases, or information systems?

Yes

- If yes: Are these digital tools, databases, or information systems new to VCC?
  - **Yes**

17.1 If you answered "yes" to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

Consult with VCC IT Services to complete a security assessment that will ensure that the initiative has reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or disposal of personal information.

Yes – IT has completed a security assessment.

- If yes, go to question 19. If you have or will complete a security assessment during the development of your initiative, you do not need to answer the question about technical security.

- If no, continue to question 18.

18. What technical and physical security do you have in place to protect personal information?

Describe where the records, whether digital or physical, for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, in a filing cabinet, etc.) and the technical and/or physical security measures in place to protect those records. (Please consult the policies for any software/cloud services/etc. but please do not just copy and paste).

- *Technical security measures include secure passwords, encryption, firewalls, etc.*
- *Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.*

- No personal information is collected in VCC's initiative.
- VCC Security for the software and device includes:
  - s. 15(1)(l)
  - Only providing access to the account ID and password to approved roles;
  - Not permitting the creation of new accounts without approval and without not using any personal information;
  - s. 15(1)(l)
  - s. 15(1)(l)
  - Following VCC Policy 505: Appropriate and Responsible Use of Educational and Information Technology.
- Eddie security measures include:
  - AXSO internal policies and procedures regarding the collection, use, disclosure, retention, and destruction of personal information, and Eddie's Privacy Policy.
  - s. 15(1)(l)

19. Controlling and tracking access

Please respond to each strategy that describes how you or your vendor limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. To effectively protect privacy, access to personal information should be limited to authorized employees who need the information to do their jobs. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information:	Yes – only approved employees will have access to the Charger account and will not provide PI
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	Yes (but no personal information collected)
We use audit logs to see who accesses a file and when:	No – because there it is a general account, access will not be tied to an individual, but there is no PI to be accessed.
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6, you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

20. How will you make sure that the personal information is accurate and complete?

FIPPA s. 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. For example: verifying information with the person it is about prior to recording it.

There should not be any personal information collected in this initiative; any personal information erroneously entered should be removed (see #21) or any account associated with an individual should be deleted.

21. Requests for correction

FIPPA s. 29 gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

21.1 Do you have a process in place to correct personal information?

In the event that an individual does input their personal information erroneously into the software, despite the generic account, users are able to correct or update their account information (including email address, etc.) through editing the "Eddie User Account" within the software. Any personal information can be removed there, or VCC generic account information can be updated. There is a minimal risk of this occurring as name, job title, VCC phone and email address are all not personal information and are what VCC staff would be most likely to use, but it does not eliminate the risk.

In the event that an individual creates an additional Eddie account using personal information, that account can be deleted through the software and uninstalled from a mobile device. Per the Privacy Policy, VCC can contact Eddie and request the deletion of that user's personal information, the removal of an email address from the newsletter mailing list, and VCC can withdraw consent to the communication or use of any personal information.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A - Correction is possible.

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A - VCC is not disclosing any personal information to a third party in this initiative.

22. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If yes, go to question 23
- If no, skip ahead to Part 7

23. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA s. 31 requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Please consult the VCC Records Retention Schedule to assist you in answering this question.

N/A

5.1 If no, describe how you will ensure the information will be kept for a minimum of one year after it is used to make a decision that directly affects an individual.

5.2 [Answer]

PART 7: PERSONAL INFORMATION BANKS

24. Will your initiative result in a personal information bank?

A personal information bank is a collection of personal information that is organized and retrievable by the name of the individual or an identifying number, symbol or other identifier.

No.

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

25. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response / mitigation strategies
Personal information is collected by software at registration/creation of an account.	• VCC is creating a general account, purpose-specific email, s. 15(1)(l) ; VCC staff will not provide any personal information at registration. • VCC staff will not be permitted to create their own accounts or install the software on their mobile devices. • Any additional accounts needed for future additional chargers will also require purpose-specific accounts to be created. • No staff will be permitted to log in with a third-party account (function is permitted by Eddie software). • Any personal information erroneously entered during registration may be removed or edited through the

Possible risk	Response / mitigation strategies
	software. Any accounts created aside from the generic account that use PI can be deleted and removed per Privacy Policy. • Any personal information that could be erroneously entered into the account is low-risk and would likely be VCC business contact information.
Software collects information on users through their interaction with and use of software, and may disclose personal information as detailed in the Privacy Policy and only in order to fulfill the purposes as detailed, including analytics and Cookies.	• s. 15(1)(l) [redacted] • The software will not be installed on any individual employee's mobile device. • Geolocation and Cookies options can be disabled.
Users may view members who accessed through the logs of charging sessions	The Charger account is not associated with an individual and ensures that no employee activities can be monitored.
Software contains hyperlinks that may direct users to websites of service providers or other third parties; the content available through those hyperlinks is not approved or endorsed by AXSO and is not governed by AXSO policies, and could expose users to potential collection of information or other risks.	Software will only be used to monitor the charging station; users should not be accessing any other content through the software or using the mobile device for any purpose other than monitoring the Charger.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to the Privacy Office for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer	Surinder Aulakh	Surinder Aulakh Digitally signed by Surinder Aulakh Date: 2024.09.11 07:36:42 -07'00'	September 11, 2024

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Brett Griffiths, Dean, School of Trades, Technology and Design		September 11, 2024
Contact Responsible for Systems Maintenance and/or Security *Only required if they have been involved in the PIA*	Norman Chang (IT)	Norman Chang Digitally signed by Norman Chang Date: 2024.09.11 14:26:04 -07'00'	Sept 11, 2024