Privacy Impact Assessment (PIA) for [ClickUp: Project Management for M&C]

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.

PART 1: GENERAL INFORMATION

PIA file number: 2024-009

Initiative title:	ClickUp: Project Management for M&C
VCC Department / Program Area:	Marketing and Communications
Link to VCC initiative website:	n/a
Link to vendor website:	https://clickup.com/
Link to vendor privacy policy:	https://clickup.com/terms/privacy
Your name and title:	Ariele Taylor, Associate Director, Client Services & Strategic Initiatives
Your work phone and email:	604.871.7159 | ataylor@vcc.ca
Initiative Lead name and title:	Danielle Libonati, Manager, Marketing and Brand
Initiative Lead phone and email:	604.871.7531 | E: dlibonati@vcc.ca

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 Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No

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.

From our GEGIT Application...

> We are requesting approval to subscribe to ClickUp, a robust, web-based project management and productivity software, for our Marketing and Communications team.
>
> By adopting ClickUp, we aim to optimize productivity and improve communication both internal and external to our department.
>
> We propose integrating ClickUp into our workflow to enhance our operational efficiency and collaboration capabilities. ClickUp, a versatile web-based platform, offers extensive customization and automation options tailored to our team's specific requirements.
>
> We envision utilizing ClickUp across various facets of our operations, including project and event planning, task assignment and management, process streamlining, reporting, and facilitating brainstorming sessions. Its seamless integration potential with our existing approved tools, alongside Sharepoint as our primary data source, ensures continuity, and enhances data management efficiency.
>
> We are currently using Basecamp as our PM tool, however ClickUp surpasses Basecamp by offering highly customizable task management tools essential for efficient task setting, collaboration, and reporting. It provides advanced custom reporting capabilities and permission-based areas for vendor and client collaboration, crucial for managing intricate projects and ensuring accountability within our larger team.
>
> These are the most common uses of the tool:

- Account registration: business contact information only (we will advise teams not to use their personal contact info for this).
- Payment information (monthly payments by VCC credit card); IP address (in Privacy Policy).
- Project management tasks, deadlines, and assignees (Employee names)
- Team comments and questions related to task status and approvals. Proofing comments.
- Brainstorming whiteboards
- Reports on work progress and status, grouped by team, employee, or client
- Images intended for marketing usage, could be from events, or procurement imagery for marketing. All images we have permission to share publicly.
- Drafted design files for marketing collateral could include public biographies or stories of various staff or partners
- Vendor quotes for various products or services
- While it is not a requirement, some team members may choose to use the mobile app on their personal cell phones.
- In the future, we may add budgeting information (VCC budgets only, not individuals)

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?

n/a not part of a larger initiative. Just adoption of a new PM software for our day-to-day operations.

Note that this tool includes the option for AI features, but we are not paying for that service at this time.

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.*

The tool would capture our daily tasks and assignments, as input by our team. We would also upload draft copies of reports and documents for design – all of these designed docs are intended for a public audience, so the risk is low if exposed. In some cases, we may invite an external project partner (ex. Vendor, collaborator) to view certain projects, but this would be granted as guest access where we can limit what information they are able to view/edit.

The potential for personal information to be collected, used, disclosed includes:

- Account registration: business contact information only (we will advise teams not to use their personal contact info for this).
- Payment information (monthly payments by VCC credit card);
- IP address (as noted in Privacy Policy)
- Images intended for marketing usage, could be from events, or procured imagery for marketing
- Public biographies or stories of various staff, students, donors, or alumni
- While it is not a requirement, some team members may choose to use the mobile app on their personal cell phones.

Ways we do not intend to use the tool:

- Sharing contact lists or additional information not listed above about students, personal staff contacts, or donor/alumni contacts

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.*

Yes

- If yes, are all of the personal information elements **necessary** for your initiative?

  Yes, 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.

As part of our team's onboarding process to the tool, we will share the definition of personal information, and direct that this tool is not to be used for that purpose. The managers of this team are also quite privy to FOIPPA regulations and will monitor for any new activities on the platform which could include personal info.

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
Scenario 1			
Step 1: VCC Registers their account, using a VCC credit card, employee names and employee emails.	Collection	26(c)	
Step 2: Monthly charges occur to the registered CC	Use	32(a)	If website is hacked, CC info could be targeted.
Scenario 2			
Step 1: VCC Staff member uses the platform from their work or home location, which provides a trackable IP address to the vendor	Collection	26(c)	Typically this is not a concern for staff. However, staff can feel free to use DaaS to access the service.
Scenario 3			
Step 1: Employee uploads a file containing VCC-owned image(s) picturing one or more individuals. Permission obtained through event photo release waiver or signed waiver for creative projects (image below)	Collection & Use	26(c) & 32(a&b)	Website is hacked and photo is used by 3rd party.

VANCOUVER COMMUNITY COLLEGE

Photo/Video Release

Marketing & Communications Department
1155 East Broadway
Vancouver, BC V5T 4V5
Phone 604.871.7000, Ext. 7188

I authorize Vancouver Community College ("VCC"), its employees and agents to:

- *photograph, film, videotape, and otherwise reproduce my likeness; digitally manipulate my likeness;*
- *publish, exhibit and otherwise use or cause to be used my likeness in any manner whatsoever that VCC deems appropriate, including publication on the internet, without payment to me.*

I acknowledge and agree that:

- *all intellectual property rights arising from the use of my likeness, including copyright and performer's rights, shall be immediately and automatically assigned to VCC;*
- *I have waived any moral rights regarding the use of my likeness in favour of VCC;*
- *all material VCC produced using my likeness shall be the sole property of VCC;*
- *this Release Form sets forth the entire agreement between VCC and myself, and no amendment to this Release Form shall be effective unless signed by both VCC and myself.*

Scenario 4			
Step 1: Biographies or stories of individuals are shared within the platform as uploads or comments to build out a document. All information would be sourced publicly,	Collection & Use	26(c) & 32(a&b)	Low risk as permission would be granted to share, or information

Scenario 4			
and/or have permission from the individual to share in VCCs marketing materials ('permission' looks different across different cases, ex. Signed form vs email approval)			can be found publicly already.
Scenario 5 (optional to employee)			
Step 1: Employee downloads the ClickUp app onto their personal phone	n/a?	n/a?	Employee takes personal risk over downloading an app not managed by VCC
Step 2: Employee engages in activities as listed above from their personal device	Use	32(a)	Hack or unauthorized use of an employees personal phone could expose our information to the third party.

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].

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]

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?

Yes, any of the information noted above in question 5 (repeated here) could be stored outside of canada ("*Your data, including personal data that we collect from you, may be transferred to, stored at and processed by us and other third parties outside the country in which you reside, including, but not limited to the United States*")

Data we have identified includes:

- Account registration: business contact information only (we will advise teams not to use their personal contact info for this).
- Payment information (monthly payments by VCC credit card);
- IP address (as noted in Privacy Policy)
- Images intended for marketing usage, could be from events, or procured imagery for marketing
- Public biographies or stories of various staff, students, donors, or alumni

- 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).

California, United States

From Clickup Privacy policy:

Your data, including personal data that we collect from you, may be transferred to, stored at and processed by us and other third parties outside the country in which you reside, including, but not limited to the United States, where data protection and privacy regulations may not offer the same level of protection as in other parts of the world. By using our platform, you agree to this transfer, storing or processing subject to the terms of our Data Protection Addendum. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this policy. Except as otherwise provided in our Data Protection Addendum, your team's project and task data will never be transferred to third parties. The only data we share with third parties is for analytics, error tracking, and marketing.

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.

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.

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

- 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.*

s. 15(1)(l)

VCC Technical and Physical: 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
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	Yes
We use audit logs to see who accesses a file and when:	Request by management team
Describe any additional controls:	Managers have the ability to change or revoke access to any individual on our account at any time.

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.

Upon being made aware of any inaccuracies in stories or individual info, we always correct them, but this relates more to our marketing best practices than to the PI for this tool. VCC is responsible for updating and changing information belonging to end users.

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?

Yes

- If yes: Please describe the process.

- Would correspond by email and make the correction as needed. VCC is able to edit information within the ClickUp platform.

From the ClickUp Privacy Policy:

- "Customers have the right to request the restriction of certain uses and disclosures of personally identifiable information as follows. You can contact us in order to (1) update or correct your personally identifiable information, (2) change your preferences with respect to communications and other information you receive from us, or (3) delete the personally identifiable information maintained about you in our systems (subject to the following paragraph), up to and including by deleting your team. Such updates, corrections, changes and deletions will have no effect on other information that we maintain, or information that we have provided to third parties in accordance with this Privacy Policy prior to such update, correction, change or deletion. To protect your privacy and security, we may take reasonable steps (such as requesting a unique password) to verify your identity before granting you profile access or making corrections. You are responsible for maintaining the secrecy of your unique password and account information at all times.
- You should be aware that it is not technologically possible to remove each and every record of the information you have provided to us from our system. The need to back up our systems to protect information from inadvertent loss means that a copy of in a non-erasable form that will be difficult or impossible for us to locate. Promptly after receiving your request, all personal information stored in databases we actively use, and other readily searchable media will be updated, corrected, changed or deleted, as appropriate, as soon as and to the extent reasonably and technically practicable."

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?

Yes – We will maintain a log document in our SharePoint files for ClickUp to record these instances.

For internal reference, it will be saved here: s. 15(1)(l)

s. 15(1)(l)

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?

Yes – we will make these attempts and record the details in the same document noted in 21.2.

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.

[Answer: Yes or No]

- 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.
    - [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**
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

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

[Answer]

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: 2024.08.26 07:47:28 -07'00'	2024/08/26

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:

[Answer]

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Ariele Taylor, Associate Director, Client Services & Strategic Initiatives Marketing & Communications	Digitally signed by Ariele Taylor Date: 2024.08.27 14:02:36 -07'00'	8/27/2024
Contact Responsible for Systems Maintenance and/or Security *Only required if they have been involved in the PIA*	Norman Chang	Norman Chang Digitally signed by Norman Chang Date: 2024.08.27 11:43:14 -07'00'	8/27/2024