Privacy Impact Assessment (PIA) for Zenoti

PART 1: GENERAL INFORMATION

PIA file number: 2024-005

Initiative title:	Zenoti – Salon & Spa Management Software
VCC Department / Program Area:	Hair Design Esthetics & Spa Therapy
Link to VCC initiative website:	https://vcc.zenoti.com/webstoreNew/services
Link to vendor website:	https://www.zenoti.com
Link to vendor privacy policy:	https://www.zenoti.com/trust/privacy-notice
Your name and title:	Norman Chang & Mary Corbett
Your work phone and email:	nchang@vcc.ca marcorbett@vcc.ca
Initiative Lead name and title:	Melanie Burke
Initiative Lead phone and email:	mburke@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: BCNET PIA 2017 BCNET AWS PIA.	

1. What is the initiative?

Zenoti is a cloud-based enterprise platform for salon & spa appointments, bookings, and management of wellness spaces, including payment for services. This platform will be used in the VCC Salon & Spa for:

- Client profile creation and client management
- Appointment booking, tracking clients' service history, and client marketing services
- Employee profile creation and scheduling
- Inventory management
- Gift card purchasing (payment in Zenoti)
- Mobile app (including client feedback feature).

Zenoti replaced the VCC Salon & Spa's previous platform. VCC Salon & Spa students, VCC staff and faculty, and members of the public who may use the Salon & Spa's services will all be users of this initiative. Salon & Spa employees consist of VCC faculty, staff, and students in the Hairstylist and Skin and Body Therapy programs, and clients could be any College members or members of the public.

Soham Inc., dba Zenoti, is a Bellevue, Washington-based company with an office in Port Moody, BC.

2. What is the scope of the PIA?

This PIA covers the full Zenoti implementation. The responses within this PIA should assist in analyzing the possible impacts on employee, customer and student privacy, describing privacy design techniques and risk mitigation measures in place as a part of the solution and ensuring that privacy considerations

are first and foremost in the design of the proposed system and within the project overall. Out of scope includes: custom development, Banner integration, partner integration, loyalty and rewards, and AI Bot.

Zenoti uses Adyen and Moneris as sub-processors/backend payment processors in Canada; they are outside the scope of this PIA. Adyen is a PCI DSS Level 1 Service Provider with PCI DSS compliance assessed by an independent Qualified Security Assessor annually.

At this time, the Salon & Spa is not using the option of self-service payment for clients through the mobile app and does not plan to implement this feature in the near future. Clients may purchase gift cards through Zenoti but not Salon & Spa services. The Salon & Spa has disabled the functions to store any credit card information, and for users to input their credit card information, in the mobile POS and mobile app.

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

Group	Data/Information Elements	Source
Employees (Faculty & Staff)	• First name, last name • VCC email • Job title, role • Work schedule • Phone number (optional, if also patrons)	PI already collected by VCC and used to create profile or collected directly from individual.
Students	Names	PI shared from class lists for students working and learning in the Salon & Spa as a program requirement.
Clients (public, VCC faculty/staff, students, etc.)	• Full name; phone number; email • Opt-in option for marketing communications • History of their services/products/purchases • "Preferences" note in online booking • Client notes that may contain health and medical information collected during consultation as it relates to administering salon/spa services; • Client notes about incidents or behaviour in spa, etc. (private notes) • Waiver and consultation forms	PI collected directly from client upon registration/profile creation on Zenoti web or mobile (or booking over the phone) and during consultation before services, or through observation (for Salon behaviour). Credit card information may only be

	• Credit card/payment information: cardholder name, card number, CVC, expiry date (only last 4 digits of credit card number are stored in Zenoti) • Gift card recipient name and email, and message (optional open text field). • Gift card balance check: Gift card number and recipient email. • Feedback from client: star rating; option for best service component; comments (open-text)	collected through Zenoti web version. Feedback is only through mobile app. *Waivers are currently paper records but may become digital and stored collected/stored in Zenoti as the mobile app is introduced. Client consultations are currently conducted through in-person interview and only relevant information is added to client notes in Zenoti.
Mobile app	Location and device ID	PI collected directly from user's device/usage
Inventory	Inventory items and quantities.	No PI collected.

3.1 Did you list personal information in question 3?

Yes

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

  Yes (medical information, behaviour notes, etc. only collected when necessary and directly related to the Salon & Spa service the client is purchasing).

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

N/A

PART 2: COLLECTION, USE, AND DISCLOSURE

5. Collection, use, and disclosure flow

Users/Clients PI Flow	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**
Registration: Clients provide information to register with VCC Salon & Spa system online and create their profile (either online or providing booking information over phone)	Collection	26(c)	
Clients select and book Salon & Spa services (optional "preferences" note field in Zenoti booking)	Collection	26(c)	
Salon & Spa staff use client information to book appointments; assign Salon students and staff to appointments; notify staff about any relevant information before client's appointment (e.g. medical information in notes to client's file that may impact service); and confirm client's booking (communications about their appointments/services/transactions).	Use	32(a)	
Clients sign a waiver before receiving services (*soon to be digital and submitted through and stored in Zenoti)*	Collection	26(c)	
Students/Staff undertake consultation interview with clients before each service to collect any directly relevant medical/health information and make notes to file.	Collection	26(c)	Consultations may become digital forms and administered through Zenoti: staff must ensure that only the minimum amount of PI, and only information directly

			relevant to spa services, is collected.
Students/staff make any notes in file about the client following the service (behaviour, health, etc.)	Collection	26(c)	
Clients may purchase gift cards through the online profile, with recipient's name, email address, by credit card online. (Gift card recipients may receive gift card via email with purchaser's name). Payment information is disclosed to Zenoti's subprocessor.	Collection Use Disclosure	26(c) 32(a) 33(2)(d)	
Clients check gift card balances with gift card number and recipient's email address.	Use	32(a)	
Zenoti may send VCC Salon & Spa marketing communications to the client, if the client opted in.	Use	32(a)	
Client is contacted with optional feedback form (including open-text "comments" field) by Zenoti, via email or mobile app.	Use Collection	32(a) 26(e)	

Employee/Salon Student PI Flow	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**
Employees (faculty and staff) create a profile with Zenoti.	Collection	26(c)	
Employees assign roles to all staff/Salon students. Students (names) are added to the general class account ("Service Provider" role) and do not individually register or have profiles.	Use	32(a)	
Employees view clients' bookings for scheduling, and may use their information (client notes, etc.)	Use	32(a)	

for administering Salon & Spa appointments and services.			
Employees issue refunds to clients when appropriate (use of last 4 digits of credit card stored in Zenoti).	Use	32(a)	

6. Collection Notice and Consent

6. 1 Collection Notice

Collection notice:

Your personal information is collected under the authority of s. 26(c) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). Your information will be used for the purposes of creating your account and administering services at the VCC Salon & Spa. If you have any questions about the collection and use of your information, please contact VCC's Privacy Office at privacyandfoi@vcc.ca.

Location: Collection notice will be provided at any point of collection (form, waiver, and on the online Zenoti account creation/registration window).

6. 2 Consent

N/A

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

Yes.

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

Zenoti is hosted on AWS infrastructure with data centers in Canada, North Virginia, Frankfurt, and Sydney.

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

Yes: Personal health or medical information

Note: Financial (credit card/payment information) is not stored by Zenoti other than the last 4 digits of a client's credit card. The Salon & Spa has disabled the setting to retain any credit card information in the mobile POS and mobile app and for clients to enter their card information. s. 15(1)(l)

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))?

No.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

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

Yes.

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Zenoti	AWS infrastructure	Data centers in North Virginia, Canada, Frankfurt, and Sydney.

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.

N/A

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

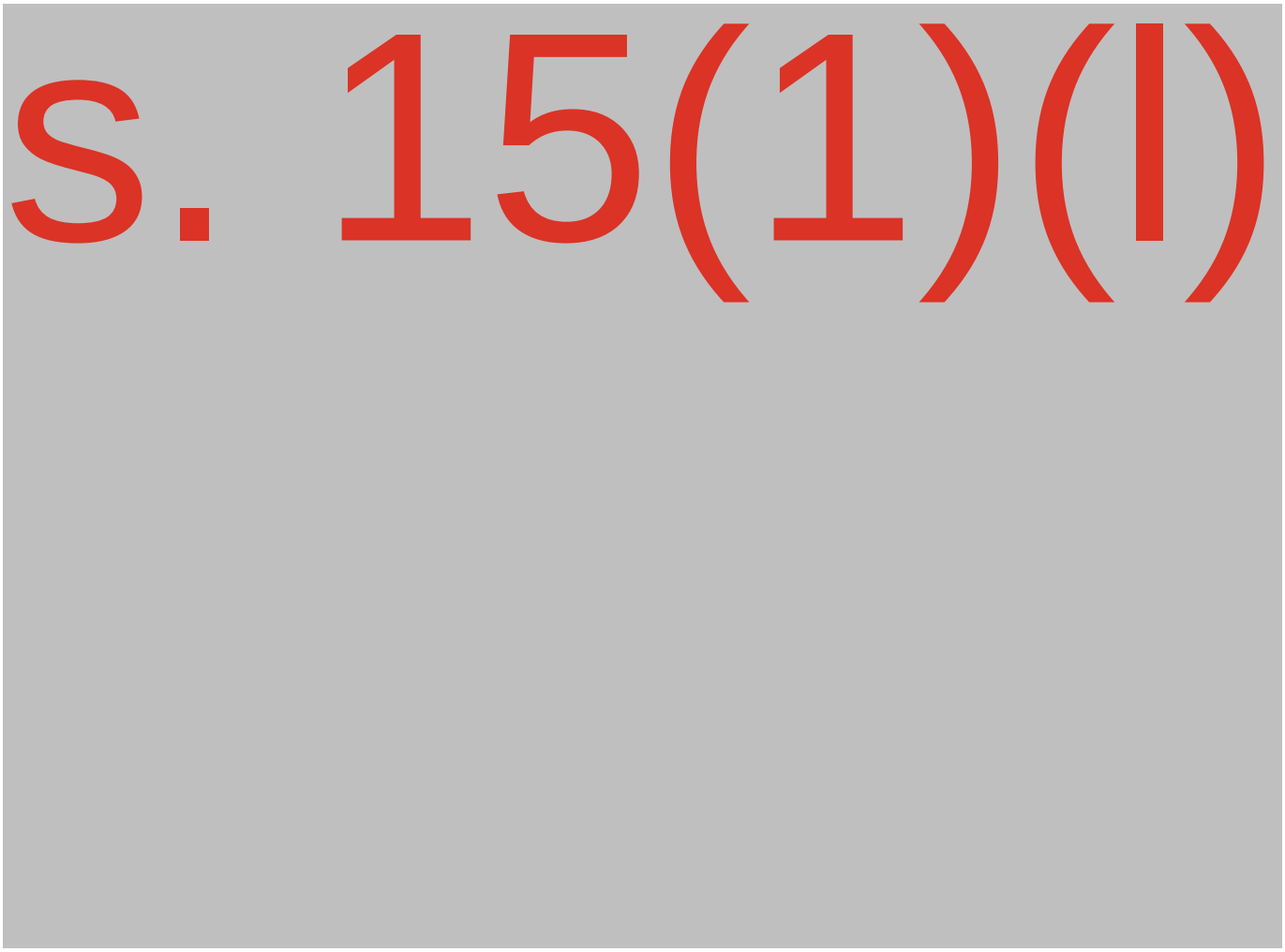
Yes – Zenoti's Terms and Conditions/Privacy Policy.

- If yes, describe the contractual measures related to your initiative.

- VCC agreed to Zenoti Services Terms and Conditions and Zenoti's Privacy Notice (Privacy Policy), last updated in 2021. This Privacy Policy (https://www.zenoti.com/trust/privacy-notice) includes information related to collection, use, cross-border transfer of information, and users' privacy rights, including access, correction, erasure, and not to be subjected to automated individual decision-making.

- Is VCC's Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative's contract?
  - No; VCC agreed to Zenoti's Terms and Conditions.

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



- VCC ensures its employees are trained and following policies related to Acceptable Use of Technology and FIPPA.

- Salon & Spa staff are trained specifically about collecting, using, and disclosing personal information in the context of delivering Salon & Spa services through Zenoti.

s. 15(1)(l)

- Employee accounts are suspended when employees leave the Salon & Spa; password to the students' class account is changed with each new class/term.
- Clients receive a collection notice before registering to use Zenoti's online services

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

s. 15(1)(l)

16. Describe the privacy risks for disclosure 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.
Hosted infrastructure is compromised.	High	Low	Medium	AWS security and technical protections.	
Users' personal information is compromised when transferred to the service provider.	High	Low	Medium	Zenoti encrypts data in transmission and at rest.	
Zenoti may transfer, process, or store personal information anywhere in the world, including but not limited to the US and India, increasing the risk that disclosure of PI may not be	Medium	High	Medium	s. 15(1)(l)	Service provider did not sign a PPS.

authorized under FIPPA, and/or that Zenoti may disclose PI without requirement to notify VCC.				Employee training: minimum amount of personal information possible is collected and any health information is directly related to Salon & Spa services (not a full history).	
VCC fails to cover aspects of PCI compliance, such as mishandling credit card data, insecure network, or lacking in security applications.	High	Medium	High	s. 15(1)(l) [redacted] training for staff using Zenoti for proper entering and storage of sensitive information.	

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? **Yes.**

PART 5: SECURITY OF 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?

Yes, for both Zenoti web and mobile app.

- If no, continue to question 18.

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

N/A - IT Security assessment completed.

19. Controlling and tracking access

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

Strategy	
We use audit logs to see who accesses a file and when:	Yes
Describe any additional controls:	Zenoti offers many options for role-based access. Salon & Spa uses select options to restrict access to personal information as needed, with these roles: • Owner: s. 15(1)(l) • Receptionist: s. 15(1)(l) • Faculty: s. 15(1)(l) • Student ("Service Provider" role): Restricted access, s. 15(1)(l) Faculty/staff accounts' access is suspended if when they no longer work at the Salon & Spa.

PART 6: ACCURACY, CORRECTION AND RETENTION

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

- Client profile/account information is collected directly from the client and made available in client's self-service portal. Only issues with clients' behaviour in Salon & Spa are collected through observation.
- Employees conduct consultation interviews with clients at each appointment to ensure that medical, health, and other personal information is accurate (notes are made in file about relevant information) .

21. Requests for correction

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

Yes: Self-service information in Zenoti can be edited by the individual (Salon employees and Clients, but not Student "Service Provider" account), and any other requests for correction can be submitted to the Salon & Spa.

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: Salon staff can add or edit notes on a client's profile if the information itself cannot be corrected.

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 but unlikely to occur: no personal information should be disclosed to another public body or third party, other than the recipient of a gift card with the purchaser's consent.

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

Yes.

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?

No: There is currently no classification for Salon & Spa client files.

- 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.

Salon & Spa is aware of their obligations to retain personal information used to make a decision about an individual for a minimum of 1 year and will not delete any client information in this time. Salon & Spa will determine a retention period for client files that considers the frequency with which people visit the Salon & Spa and the need not to retain sensitive personal information longer than necessary.

PART 7: PERSONAL INFORMATION BANKS

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

Yes: Client profiles/files are searchable by clients' name or phone number in the system.

PART 8: ADDITIONAL RISKS

25. Risk response

Possible risk	Response / mitigation strategies
Risk 1: Unauthorized access, use, or disclosure of clients' personal information by Employees/Salon students.	Employees and Salon students receive FIPPA training and understanding of policies and confidentiality requirements. Role-based access implemented to limit access to personal information to need-to-know basis.
Risk 2: Students have continued access to Zenoti system through one "Service Provider" account.	Unique password for each Salon & Spa class will be used, so that students will not have access to Zenoti/client files past the end of their program.

PART 9: SIGNATURES

Privacy Office Comments

The Salon & Spa has changed the default setting for marketing communications in Zenoti to be that clients must opt-in. This PIA should also be revised if the Salon & Spa requires any other personal information to be collected, such as elements related to loyalty and rewards functions or other marketing purposes.

The Salon & Spa does not intend to use the self-service payment option for services through the mobile app at this time. If the Salon & Spa uses that option in the future, the PIA should be revised to include that feature.

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: 2024.12.18 05:54:49 -08'00'	Dec 18, 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.

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Melanie Burke, ADH Salon & Spa	Melanie Burke Digitally signed by Melanie Burke Date: 2025.01.07 09:42:00 -08'00'	Jan 7, 2025

Role	Name/Position	Electronic signature	Date signed
Contact Responsible for Systems Maintenance and/or Security	Norman Chang Director IT	Norman Chang Digitally signed by Norman Chang Date: 2025.01.06 12:52:26 -08'00'	Jan 6, 2025