VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

[Department and Project Name]

Part 1 - General

Name of Department:	Student Affairs / DEHR / UNSEC / General Counsel		
PIA Drafter:	Janelle LaCroix		
Email:	Janelle.LaCroix@viu.ca	**Phone:**	
Program Manager:			
Email:		**Phone:**	

1. Description of the Initiative

VIU is considering the purchase of Maxient case management software. The primary application of the software is the management of Conduct and Care (student conduct), Accessibility Services and DEHR cases as well as sexual misconduct reporting and case management.

2. Scope of this PIA

This PIA assesses:

A. The privacy risks associated with the use of Maxient software by all interested departments, including the collection, use, storage, disposal and disclosure (intentional or otherwise) of VIU community members' personal information and sensitive personal information;
B. The suitability of the software, from a privacy perspective, for use in a legal case management capacity. The latter application involves privileged legal communications which may include the personal information and sensitive personal information of VIU employees, students, contractors, volunteers and non-VIU community members.

3. Related Privacy Impact Assessments

None

4. Elements of Information or Data

Information Type	Information Collected
Personal Information collected by Student Affairs, Legal Services and the DEHR (collectively)	**From Students:** - Name - Student number - Date of birth - Mailing address - Email address - Phone number(s) - Program of Study - Photo - Emergency contact info - Current course schedule

	- Course enrollment history (including grades) - Flags on student record - International student status - Indigenous student status - Gender (self-identified) - Personal details that would be provided in a discrimination and student conduct complaints, as well as human rights and labour relations matters (relationships, family matters, mental health information, etc.) **From Third Parties:** - In limited circumstances, Conduct and Care will create a student profile and number for non-students or prospective students using their name and contact for the purpose of flagging that person for health/safety reasons. - In the DEHR and in Conduct and Care, where complaints involve allegations of sexual misconduct against non-VIU community members, or where there are witnesses to investigations who are not VIU community members, a potentially broad range of their personal information could be collected. **From VIU Employees:** - Where VIU employees are complainants or respondents to complaints, or where they report a student conduct issue to conduct and care, they may be required to provide personal information such as their home address, personal email address, or a broad range of personal information and sensitive personal information in the case of sexual misconduct matters.
Sensitive Personal Information collected by Student Affairs, Legal Services and the DEHR (collectively):	**From Students, Third Parties and VIU Employees:** - Information relayed by way of Sexual Misconduct complaints or responses to same (sexual conduct, experiences, trauma, history, health, etc.) - Information relayed in discrimination complaints (sexual orientation, preference or identity, sexual health information, psychological history) - Information related to disability (medical diagnoses and history) and accommodations.
Contact details	**From Students:** Personal contact and emergency contact info **From Third Parties:** Phone numbers of emergency contacts (personal or business) **From VIU Employees:** Business and personal contact information
Account information	**N/A**

Commercial information	In terms of commercial contracts and litigation files, General Counsel's Office will collect and store commercial information where business entities are involved in matters with VIU.

*If personal information **is** involved in your initiative, please continue to the next page to complete your PIA.*

*If **no** personal information is involved, please submit Parts 1, 6, and 7 unsigned to fippa@viu.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.*

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada: Maxient provides Canadians with the option to store all data in Canada. VIU's contract with Maxient should stipulate that this will be the case.

6. Sensitive Personal Information: Does the project/initiative involve very sensitive personal information? Examples of sensitive personal information include personal health information, genetic and biometric data, personal financial information, geolocation data, criminal records, counselling records, HR records and payroll records. **If so,** will the sensitive personal information collected be stored outside of Canada?

Yes, sensitive personal information will be collected – no, it will not be stored outside of Canada.

7. Data-linking Initiative*

This is not considered a data-linking initiative as contemplated in s.36.1 of FIPPA.

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

8. Common or Integrated Program or Activity*

This initiative is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
This initiative involves a program or activity that provides a service (or services);	
Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	
The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

9. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table				
	Description/Purpose	**Personal Information**	**Type (Collection, Use or Retention)**	**FIPPA Authority**
1.	Demographic and personal contact information from students	Yes	All	26(c) 32
2.	Demographic information collected from employees	Yes	All	26(c) 32
3.	Information arising in the course of student conduct, accessibility services and sexual misconduct files regarding students, employees and third parties	Yes	All	26(c) 32
4.	Information arising in the course of DEHR files regarding students, employees and third parties	Yes	All	26(c) 32
5.	Details of legal matters potentially involving VIU community members and third parties.	Yes (possibly)	All	26(c) 32

10. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Unauthorized Collection of PI	• Use of predetermined data fields. • Security/log-in access and tracking to limit employees with access and time/date track use. • Employee privacy training	Low	High
2.	Unauthorized Use of or access to PI	• Security/log-in access and tracking to limit employees with access and time/date track use. • Use of Verification of Identity and Authorization Protocols where records are requested • Employee privacy training	Low	High
3.	Unauthorized Disclosure of PI	• Reporting by any VIU community member of privacy concerns; privacy breach management protocol; human resources conduct investigations. • Use of Verification of Identity and Authorization Protocols where records are requested • Employee privacy training	Low	High

11. Collection Notice

Individual departments collecting personal information will be responsible for drafting and using their own collection notices.

Part 3 – Security of Personal Information

12. Please describe the physical security measures related to the initiative (if applicable).

Restricted access to property (i.e. key or key card access and access limited to authorized employees)
Security monitored building
Locked doors
Locked filing cabinets – used for printed/paper records
"Clean desk" practices

13. Please describe the technical security measures related to the initiative (if applicable).

From Maxient: [Note – regarding all references below to data storage in the U.S. - that Maxient will store the data of Canadian customers within Canada and approval of this PIA is subject to written confirmation of same by Maxient].

s. 15(1)(l)

[redacted]

…

[redacted]

…

Beyond the physical security at our datacenters, we take several other measures to improve security. [redacted]

s. 15(1)(l)

[redacted]

As part of your contract with Maxient, all of your data will automatically be backed up nightly, [redacted]

Several other security measures, both minor and major, are in place which we do not disclose publicly.

...

[redacted]

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

See the responses to items 12 and 13, above.

15. Please describe how you track who has access to the personal information.

See the response to item 13 above (authenticating users).

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

The correction or updating of individuals' personal information will occur in accordance with VIU's *Correction of Personal Information Best Practices Guide*.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

In some cases, decisions regarding student conduct matters, DEHR complaints and General Counsel matters will rely on the use of personal information.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

To the greatest extent possible and in keeping with privacy best practices, personal information will be collected directly from the person to whom it pertains, which will increase accuracy. To the extent that decisions are based on personal information that is incorrect, the holders of the personal information will have an opportunity to either make corrections to the decision, or to appeal it under VIU policy and procedure.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

VIU has engaged the services of an external privacy consultant and it is expected that the University will have a records retention and disposition schedule by the end of 2023. In the meantime, records are retained and disposed of pursuant to the pertinent regulation/authority.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No – other than the transfer of data to Maxient from the University in the ordinary course of using the software (i.e. via data feeds).

21. Access for Research or Statistical Purposes: Will the information collected be used for research or statistical purposes?

Users of the software may avail themselves of reporting features of the software, but at the time of this writing, there is no plan or authorization in place to collect or use information for research purposes.

Privacy Impact Assessment for:

[Department and Project Name]