VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Prismatic Data Solutions:

Return to Work (RTW) Management Module

Part 1 - General

Department:	Health and Safety / Human Resources	
PIA Drafter(s):	**Erin Bascom**, Health & Safety Advisor	Erin.Bascom@viu.ca
Contributors:	**Josephine McNeilly**, Specialist, Health, Well-Being, and Benefits	Josephine.Mcneilly@viu.ca
	Mike Culbertson, FOI & Privacy Officer	Privacy.Officer@viu.ca

1. Description of the Initiative

The proposed Return-to-Work (RTW) module is an add-on to the existing Prismatic Data Solutions Safety Spectrum Incident Management Software system implemented in summer 2023 for Health and Safety Incident Reporting. The RTW module would integrate with the incident reporting system to help facilitate, track, and manage Occupational Leave (OL) and Non-Occupational Leave (NOL) claims. Currently, OL and NOL claims are managed jointly between Human Resources (HR) and Health and Safety Services (HSS) with a variety of tools and communication channels. The RTW module would centralize case management with all case-related communications, updates, incident reports, return to work plans, medical documents, etc.

The addition of the RTW module would ensure workers are supported in the most efficient and effective way possible during all types of illness/injury leave. It includes additional benefits for HR and HSS with more efficient integrated data sharing, tracking, task automation and improved data security, as recommended by VIU's recent NIDMAR audit, to increase evidence-based practice and reduce costs.

For more details about this initiative, please see the Briefing Note saved on file with this PIA.

2. Scope of this PIA

This PIA addresses privacy implications in the Prismatic Return to Work Management Module specifically as well as the privacy practices of Prismatic in general. It will also consider how VIU will use the software while managing and protecting personal information of its clients (VIU Employees).

Additional modules or significant changes to how personal information is collected, used, or disclosed would require an addendum or additional PIA.

3. Related Privacy Impact Assessments

Prismatic Data Solutions Safety Spectrum Incident Management Software [redacted]. The PIA for the Prismatic Incident Management software was done by [redacted]. The VIU privacy officer at the time was satisfied that it met VIU's privacy obligations under FIPPA. s. 21(1)

4. Elements of Information or Data

Personal Information: list any recorded information about an identifiable individual other than contact information.	**From Students**: N/A The RTW module applies to VIU employees. **From Third Parties**: N/A The RTW module applies to VIU employees. **From VIU Employees**: Both IR and RTW modules[1] • Employee ID • Employment Status • Email • Job Title ID / Position ID • Location • Department ID • Department Name • Supervisor Employee ID • Username • Wage details and personal home information[2] • Social Insurance Number (SIN)[3]

[1] As part of the Prismatic Incident Reporting (IR) module (separate PIA) Prismatic integrates with the VIU Enterprise Resource Planning (ERP) system, Unit 4, via API and collects the information listed in box one from all VIU employees. Prismatic and VIU ERP systems are synchronized once every 24 hours. The RTW module also utilizes the information collected from the IR module.

[2] This information is collected during the IR phase on a separate form (form 7) only when medical treatment and time loss incidents occur. It may be stored in a case file in the RTW module.

[3] The SIN is pulled in from unit 4 in the IR module only for WCB form 7 submissions but is forgotten by the system after 24 hours.

VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Prismatic Data Solutions:

Return to Work (RTW) Management Module

Personal Information collected and used only in RTW module	• All information related to the leave type, insurer, claim summaries, and return to work plans. Please see appended screen shots. • Information as required to manage Manulife insurance claims (See example on file). • Temporary Abilities and/or restrictions • Medical Documents • OL: Doctor's notes • NOL: Independent Medical evaluations • Personal Health Numbers (PHN): VIU does not intentionally collect PHNs, however, they may inadvertently collected in correspondence, which is stored in the RTW module. • OL: WCB claim appeals. They are infrequent but we manage them. They include full claim disclosure from WCB. The claim disclosure includes a section on medical documents. I reviewed the one active appeal we have now, and those documents do include PHN's. The medical documents there include: • Physicians report – have the PHN • Physicians' assessment or work abilities (see example on file) • WCB medical referrals – have the PHN • Progress reports for healthcare practitioners – no PHN • Invoices submitted and letters about invoices – have the PHN • Medical Treatment Plans
Contact details (collected in IR module; used in both IR/RTW)	From Students: N/A The RTW module applies to VIU employees. From Third Parties: N/A The RTW module applies to VIU employees. **From VIU Employees:** • First Name • Preferred Name • Last Name

	• Job Title / Position Name
Account information	
Commercial information	Standard VIU business information would be shared to facilitate the purchasing transaction.

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

- All client infrastructure is hosted with [redacted]. Each client gets their own separate infrastructure that is not shared with anyone else.

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?**

s. 15(1)(l)

- Yes: personal health information as well as HR and payroll records. The sensitive personal information will be stored on [redacted].

7. Data-linking Initiative*

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

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.

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

Description/Purpose 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.	**Type (Collection, Use, or Disclosure)**	**FIPPA Authority**
An authorized worker logs into the Prismatic software with credentials using Single Sign On and Multifactor Authentication (MFA).	N/A	
The authorized worker opens the RTW module and manually starts a new case for an employee who is off work due to NOL/OL.	Use	26(a)
Once the case window opens the case summary page is completed. This includes categories 1-6 of information: 1.Case type: - Case title - Case type (RTW or stay at work) - Payee status (no wage info collected, it is just a status)	Use Disclosure	32 (a) 33.2 (d)
2. People: - Employees away from work are called involved or injured employees. They are selected using the person selector, which draws from the main Prismatic software database that is also used for the Incident Reporting module. Employee information is synchronized with the VIU ERP database (Unit 4) each evening and includes data in section four above. This data disclosure was covered in the Prismatic Incident Reporting module PIA. While there is additional data in the system from the IR module, only two items are displayed in the return-to-work module for authorized users to view: - Involved employee name - Involved employee supervisor name	Use	32 (a)

Authorized VIU employees directly enter the information in items 3-6: 3. Other people - insurance provider - worker representative (not required) - Employer representative (not required)	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
4. Work Status (NOL/OL, at work or home, last day worked, first shift missed, estimated or actual RTW date)	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
5. Current Plan (for active RTW plans near the end of the case)	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
6. Non-work related injury or illness details (this is for NOL, which are not started in the IR module.	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
Other folders in a case for information are: Communication logs, Medical Documents, Capabilities, Meetings, Case Plans and Closure.	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
As a case evolves over time data is entered into and stored electronically in these other tabs. The data entered or stored is used to manage cases and correspondence and to return employees to the workplace.	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
The other data entered or stored in the system may come from email, phone calls, meetings, doctors and other health care professionals, insurers, or the workers compensation board of BC.	Collection Use Disclosure	26 (c) 32 (a) 33.2 (d)
The data is stored by Prismatic software who uses [redacted] which is cloud based and stored in [redacted] Canada.	Use Disclosure	32 (a) 33.2 (d)
Retention		

s. 15(1)(l)

10. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized employees, contractors, or third-party vendors of Prismatic view or access the PI of VIU employees*	[redacted] s. 15(1)(l) *See Prismatic Security Policy saved on file with this PIA.	Low	High
2.	Unauthorized VIU employees access sensitive personal information	- Apply principle of least privilege using Role-based access control (RBAC) feature: give users only the privileges they need to perform authorized tasks. - Employee privacy training - Prismatic has "audit logging" – detailed logs about all activity on servers	Low	High

		available on request. Also have "track changes" feature- tracks who/when changes user settings/permissions. -VIU will use the optional MFA for higher level access where sensitive PI is involved		
3.	Data breach by hacker	[redacted] - More details about Prismatic's data security measures are described in Part 3: Security of Personal Information	Low	High

s. 15(1)(l)

11. Collection Notice

Under FIPPA section 27(2), you **must notify individuals when you collect their personal information directly from them**. Whenever possible, the collection notice should be positioned so people read or hear it before they are asked for their information. At minimum, a collection notice must contain **i.** purpose for collecting the information; **ii.** Legal authority under FIPPA or other legislation; and **iii.** Contact information of a person at VIU who can answer why you're collecting the PI, how it's used, and how people can update or correct their information.

- The IR module uses the following collection notice for incident reporting:

The information on this form is collected under the authority of the Freedom of Information and Protection of Privacy Act (R.S.B.C. 1996, c. 165). It is related directly to and needed by Vancouver Island University in order to follow up on health and safety reports and to comply with WorkSafeBC requirements. The information will be used to contact individuals who made or are referenced in the report and to initiate an incident investigation. It may also be used to facilitate the administration of a WorkSafeBC claim. If you have any questions about the collection and use of this information please contact Kim Sharpe, 900 Fifth Street, Nanaimo, BC, V9R5S5, Kim.Sharpe@viu.ca."

- For the RTW module, there is no direct collection of personal information. Personal information in the RTW module is collected from other previously collected points, for example, through IR module integration, Unit 4 integration, and from third parties such as doctors' assessments, correspondence with insurance companies, claim disclosure forms from WCB, etc. As such, a collection notice is not needed for this module.

Part 3 – Security of Personal Information

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

Please see Prismatic Data Solutions' Security Policy saved on file with this PIA for a description of their physical security measures (Section 7, pg. 8).

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

Please see Prismatic Data Solutions' Security Policy saved on file with this PIA for a description of their technical security measures (Section 4, pgs. 4-5).

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.

[redacted]

Further, only designated/authorized VIU employees will have the ability to make changes to personal information in the RTW module. s. 15(1)(l)

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

[redacted] Employee access will be reviewed periodically.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected?

FIPPA section 29 states that if a person believes there is an error or omission in their information that is in your custody or control, they can ask you to correct it.

- Any error in personal information would be in Unit 4 since the data is linked. Employees can view their data and update it inside unit 4. Those updates would transfer to Prismatic after 24 hours. Other information may be from an external insurer or medical professional, and we are just viewers of the data. They would have to go to the provider of any external documents if there was an error.

16a. If information is not updated or corrected (for physical, procedural, or other reasons) please explain how it will be annotated? If for any reason a correction is not made, their record must be annotated with their request.

- There is a Communication Log in the RTW module, and we could add a memo about the request. The note would stay on the file. If it was corrected, then we would update the memo saying it was competed and on what day.

16b. If personal information will be disclosed to others, how will VIU notify them of the update, correction or annotation?

If you've corrected or annotated a person's record, you have to notify any third party to whom you've disclosed their information.

- If we disclosed information to a third party that required a correction, we would notify the external party via applicable method for that third party. We would make a note in the communication log confirming it was done.

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

Will any of the personal information you've collected be used to make decisions about an individual? For example, will their information be used to determine if they qualify for a benefit? What type of care they receive? Change jobs? Etc.

- Yes.

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.

It is your responsibility to ensure the personal information you collect, store, use, or disclose is accurate and complete – especially if it is used to make a decision about the individual. FIPPA recommends verifying the information with the individual prior to recording it.

- Any decisions made are only be made after discussions with a worker where all information used in the decision is reviewed with them.

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?

FIPPA stipulates that any personal information that was used to make a decision about an individual is retained for at least one year after the decision so the individual has a reasonable opportunity to access that personal information.

- Health and Safety stores their records for WCB claims for 7 years as per older requirements. Now the requirements vary between 3 and 10 years depending on what the record is. Our department will look at this and update our procedures.

Part 5 – Further Information

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

- Yes, Prismatic will be integrating with VIU's HR system, [redacted] s. 15(1)(l)
- Either way, this is a routine and systematic disclosure of VIU employee personal information to Prismatic Data Solutions.

21. Will the information collected be used for research or statistical purposes?

- VIU will not use the information for research.
- VIU will use the information for statistical purposes but it is anonymized so there is no personal data included. The statistics are for internal use and will allow the employer to track things like trends, number of days missed, types of cases, absence length, accommodations as well as case open times.

Part 6 - Summary and Proponent Responsibility

Summary:

Prismatic Data Solutions meets industry standards for privacy and security as can be seen in their attached Security and Privacy Policies. This PIA covers how the software will be managed internally to mitigate risk at VIU. One of the main areas of concern is the personal information we inadvertently collect from third parties that are then stored on the platform, such as Personal Health Numbers and other personal details from medical documents. However, the department has committed to redact such information when possible, to help mitigate this risk.

Recommendations:

- Limit the collection of personal information to only what is necessary for operational requirements and routinely review the PI collected to determine the minimal needed.
- Limit the sharing/disclosure of personal information with Prismatic to only what is necessary to facilitate, track, and manage OL/NOL claims.
- Prismatic states that they have a very flexible user access and management system. Using the principle of least privilege, limit access to as few employees as possible, and only enough to perform their duties.
- Plan for removing access for outgoing employees: the operational unit has committed to monthly or quarterly review of the system users as a best practice and safeguard.
- All users will access both IR/RTW modules via multi-factor authentication (MFA)
- Plan for employees to take the VIU Privacy Training course (available February 2024).
- When possible, VIU HSS/HR will redact personal health numbers from medical documents stored in the system. Note: some of these documents come from doctors or medical evaluations and VIU will only have read-only access and may not be able to redact.
- Review the forthcoming Records and Retention schedule and make any necessary adjustments to current records retention/deletion practices. Update this PIA with any changes.

Part 7: Signatures

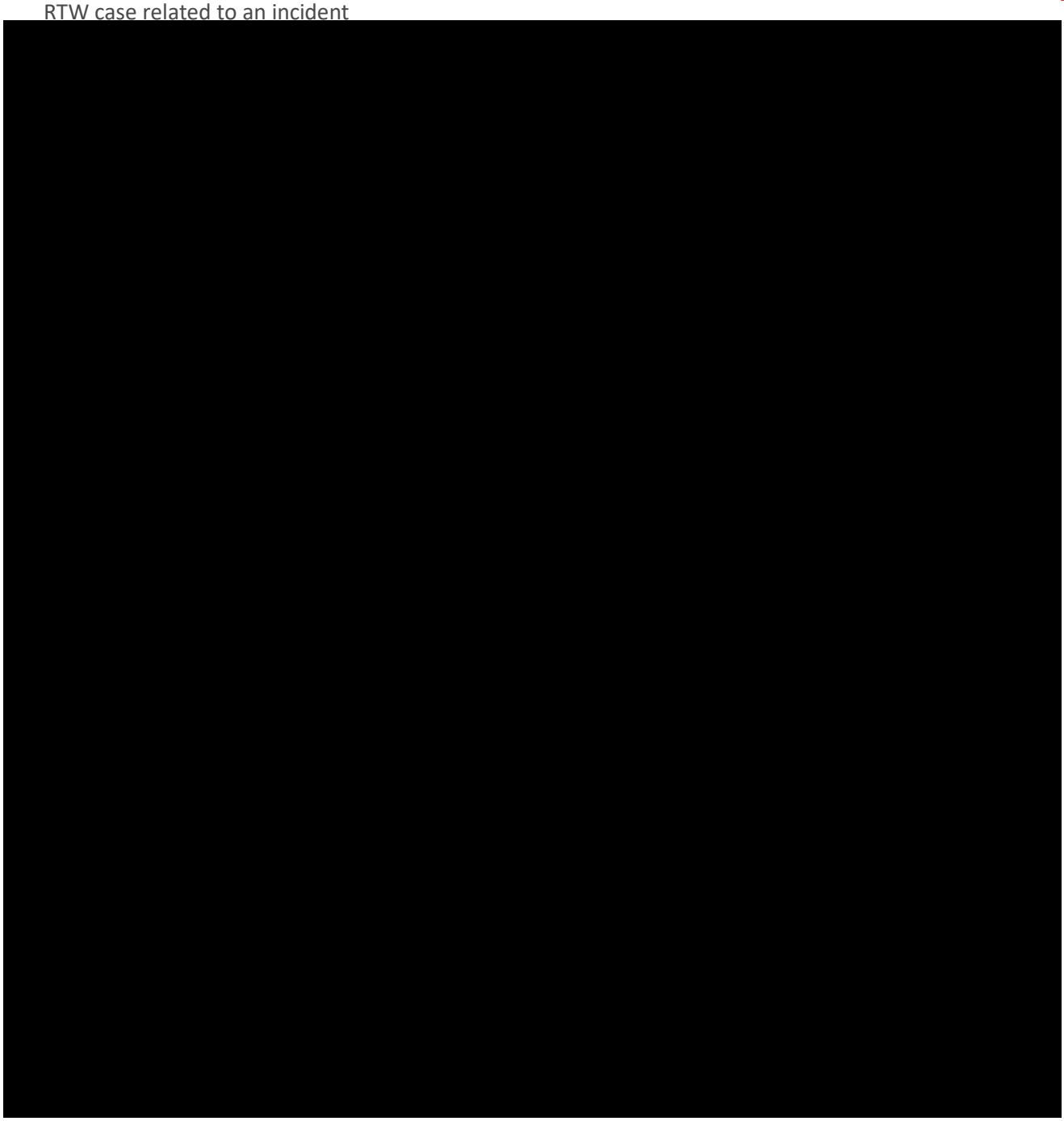
Role	Name	Electronic signature
Initiative lead		
Program/Department Manager (if different from initiative lead)		
Privacy Officer / Privacy Office Representative	**Mike Culbertson** FOI & Privacy Officer	[redacted]

s. 22(1)

s. 15(1)(l)
s. 21(1)

Appendix: RTW Module Screen Shots

RTW case related to an incident



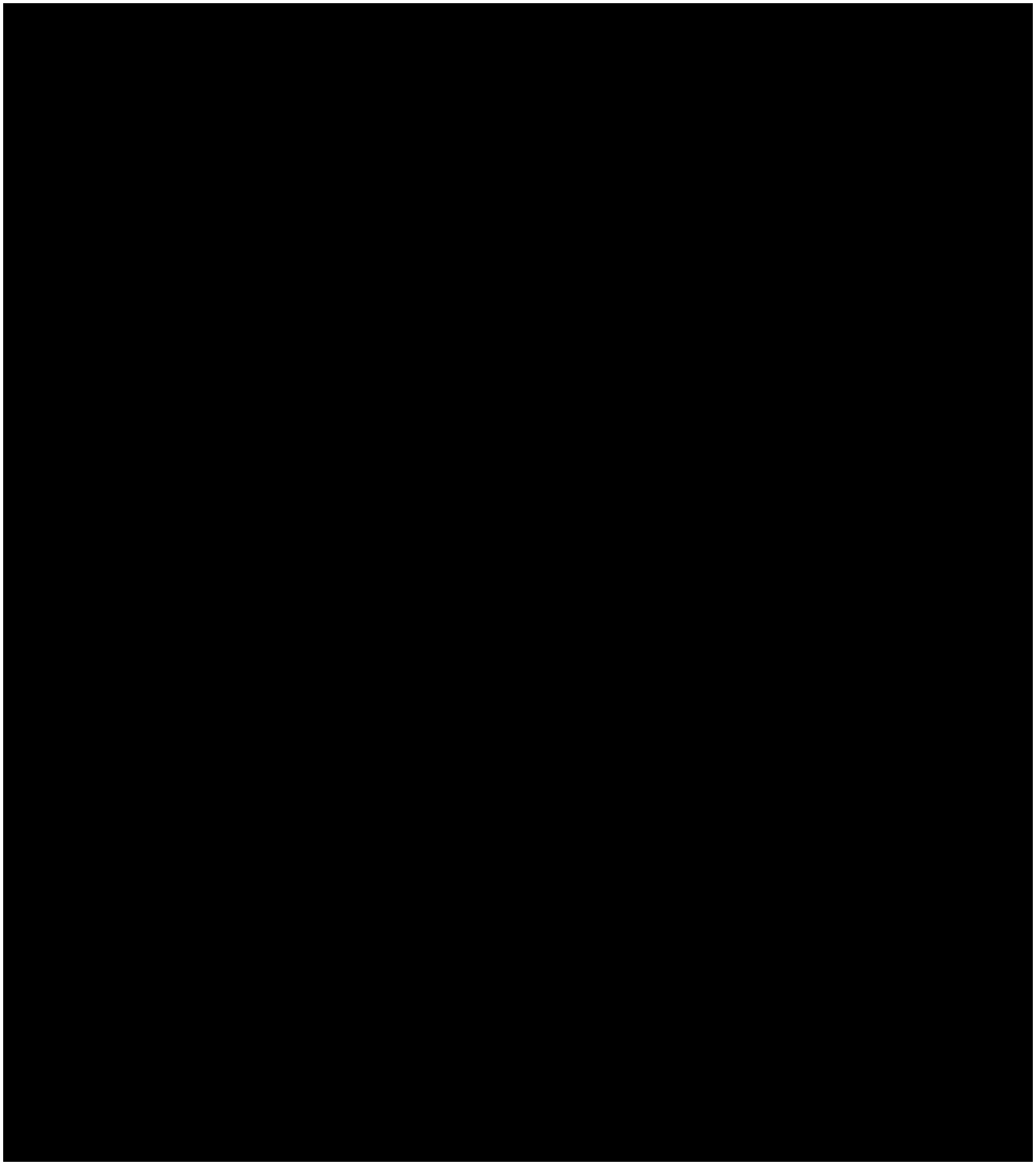
VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Prismatic Data Solutions:

Return to Work (RTW) Management Module

s. 21(1); s. 15(1)(l)



s. 15(1)(l);
s. 21(1)

[redacted]

s. 21(1); s. 15(1)(l)

[redacted]

[redacted]

[redacted]

[redacted]