

PIA # and Name- PRIVIT 23-24

1 General Information

1. Name of Department, Branch and Program Area

UNBC Athletics

2. Name of Program or Service Representative

PRIVIT

3. When will the initiative take place?

10/1/23

4. Is this a one-time event?

Yes

No

5. Do you have an end date planned?

Yes

No

6. Describe the New Program or Service or the Change.

<https://privit.com/athletics/#top>

Move from a paper system to online system that allows for our student athletes information to be stored appropriately and access designated to appropriate employees.

7. Describe the Purposes, Goals and Objectives.

- Track completion of profiles, documents and signatures with the comprehensive dashboard tools.
- Communicate status with the key people in your organization, all within PRIVIT portal.
- Field level encryption and full privacy compliance
- Give athletes, coaches, staff and athletic trainers the time to focus on success, by eliminating hours wasted filling out and managing paperwork.

8. Describe the Governance Model – who is ultimately accountable for the program or system.

Athletics Director

9. List any Relevant PIAs

NA

10. List of All Stakeholders Impacted / Involved (i.e. who are you collecting information from, UNBC roles using PI, 3rd parties with whom you will share information)

Stakeholder	Role in the initiative
UNBC Student Athletes	We collect their data digitally vs current paper system
Engage Sport North	Data collection, athletic therapy input, and utilize the mandatory information for Canada West and U SPORTS compliance (fit to play, pre season forms)
UNBC Athletics	Owner of the software and responsible for overall usage, authorize appropriate users

11. List any relevant contracts or software purchases. Be sure to follow [UNBC guidelines](#) regarding purchasing policies.

PO: VM105971

2 Collection and Use of Personal Information

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

Data Element name, email, id#, grade	Rationale for collection, use or disclosure	Method of Collection or Disclosure	FIPPA Section (completed by Privacy)
Name/contact information	Determine varsity eligibility and contact the student athletes when required.	Direct Indirect	26(c)
Personal Health #	Mandatory to have extended health coverage.	Direct Indirect	26(c)
Emergency contact	In case of an emergency.	Direct Indirect	26(c)
Medical fit to play	Mandatory for CW compliance.	Direct Indirect	26(c)
Injury/concussion status	Return to play/practice eligibility.	Direct Indirect	26(c)
		Direct Indirect	TBD
		Direct Indirect	TBD

13. Describe how [personal information](#) is to be collected

- online forms
- face to face conversation and collection

14. If you already have a collection notice, attach it as an appendix.

15. Please list all users of PI and Describe how personal information is to be used.

User (UNBC Roles e.g Governance officer)	How the info is used
Director of Athletics	Emergency contact, return to play status, U SPORTS season ending injury reporting.
Athletic Trainer	Data input for injuries, concussion reporting, pre season form compliance
Coach	Return to practice/ phases of practice clearance/ concussion stage - return to play protocol
Engage Sport North Contractor	Data input for injuries. Use information to make decisions about student athletes.
Administrator	Can view information entered into PRIVIT.
Coordinator	Can view and edit information.
PRIVIT Account Manager	Help UNBC manage the integration of PRIVIT. Will not access personal information provided. Is a coordinator and administrator.

16. Do you use personal information in your initiative to make a decision about an individual?

Yes

No

17. If yes, do you have a retention schedule in place related to personal information used to make decisions?

Yes

No

18. If yes, please your approved information schedule as an appendix.

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

Athletics will coordinate with Privacy to develop a retention schedule within the first year of the initiative.

3 Storage of Personal Information

20. Is any personal information stored outside of Canada?

Yes

No

21. Describe how PI information will be stored

For example, are *you using a cloud* storage (OneDrive), or Software as a Service (SaaS).

Servers are hosted by AWS. See HECVAT and other security documents for more in depth information.

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

Yes

No

If yes, please discuss with [UNBC Information Security](#) whether you also require a security and threat risk assessment

4 Research / Health System Use

23. Do you anticipate that data collected by this program / system will be used for research or health system use?

Yes

No

If "Yes" answer the following questions, if "No" please proceed to the next section.

24. Please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

NA

25. Will it be disclosed as part of Health System Use?

Provide details on the disclosure, including where and how personal information will be stored.

NA

26. Will it be disclosed as part of Research / Open Data?

Provide details on the disclosure, including where and how personal information will be stored.

NA

5 Disclosure

27. Will you be disclosing information to 3rd parties (i.e. non-unbc employees)?

Yes

No

If "Yes" answer the following questions, if "No" please proceed to the next section.

28. To whom will you be disclosing personal information? Provide details on the disclosure, including where and how personal information will be stored.

PRIVIT will be accessed by Engage Sport North as part of their contract as our lead Integrated Support Team for all things related to Athletic Therapy and Strength and Conditioning.

29. If personal information will be disclosed to anyone outside of Canada, provide details on the disclosure, including where and how personal information will be stored.

NA

6 Accuracy and Correction

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

The student athlete completes the personal information and further notes are then done by trained contracted professional - Athletic Therapist.

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

Yes

No

32. If yes, please describe your process below?

Super users and coordinators can make edits.

33. Describe the process of how you will make a note on the record, if you're not able to correct the record itself.

NA

34. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third-party recipient of the request for correction. How will you ensure that you conduct these notifications when necessary?

Athletics will coordinate with Privacy on appropriate steps to take when or if this scenario arises.

7 Personal Information Banks

A personal information bank is a collection of personal information that is organized or searchable by the name of the individual or an identifying number, symbol, or other identifier. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- linked to an identifiable individual
- organized and capable of being retrieved by a personal identifier
- normally compiled for a single purpose

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

Yes

No

If "Yes", answer the following questions, if "No" please proceed to the next section.

36. Describe the business purpose for the information bank (i.e., account management of clients, student record management)

The purpose would be to manage all the members of the varsity teams, having their personal and team information all in one place. This will allow coaches, athletic therapists, and the director to be able to access the information they need to make important decisions about the individual athletes and the entire team.

37. If aggregate reports are generated, explain how Personal Information will be de identified or anonymized and by whom?

NA

38. Describe the category of users and the information to which they will have access

Category of Users

Information accessed (i.e. contact info, grades, fee etc.)

Athletic Director (coordinator)

Super user. Has access to all information. Can make edits to information. Can add users and revoke access.

Athletic Trainer (coordinator)

Super user. Has access to all information. Can make edits to information. Can add users and revoke access.

PRIVIT Account Manager (coordinator)

Has access to all information. Will assist the two super users with using PRIVIT.

Coach

Will have access to the personal information of their specific team members.

Contractor (Engage Sport North)

Will have access to all information provided.

Administrator

Will have read access to all information provided.

39. Who is responsible for oversight of user access?

Athletics Director

40. Who reads the audit logs, and how long are they kept?

[Redacted]

41. What does the audit log track? How detailed is the data (e.g., date stamps, time stamps, access control number, IP address, etc.)? Does the audit log include the purpose of an access?

[Redacted]

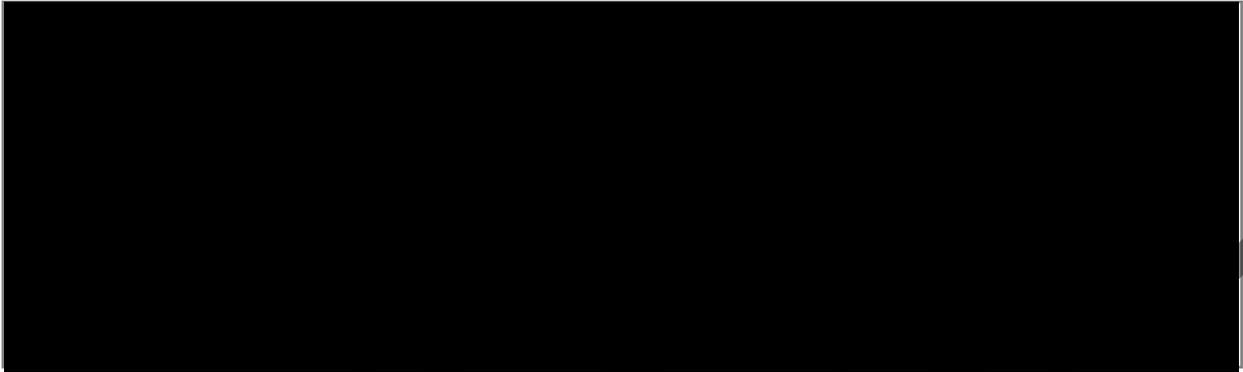
42. Are the audit logs immutable?

Yes No

43. Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs (e.g., does the auditor in the organization have a role, or is it the security department?)

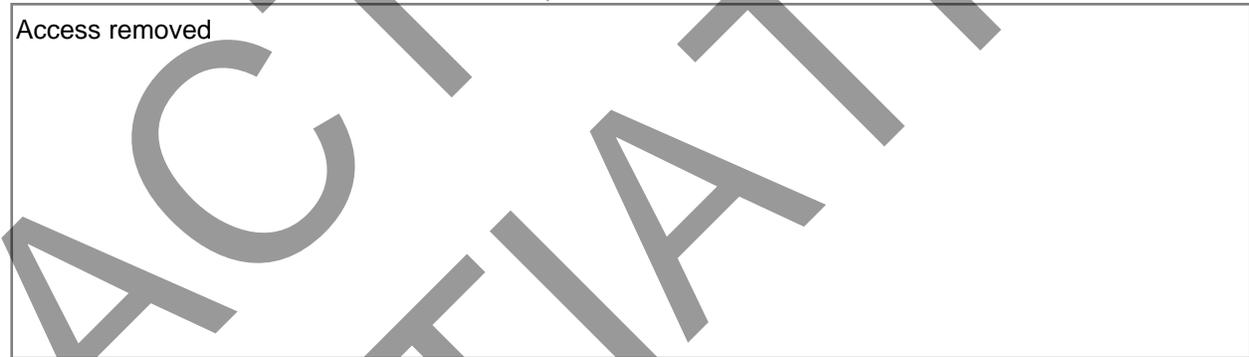
Yes No

44. Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?



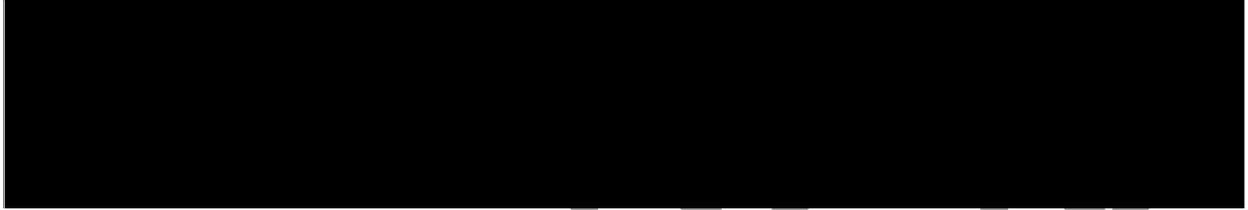
45. How will those found to abuse access privileges be sanctioned ?

Access removed



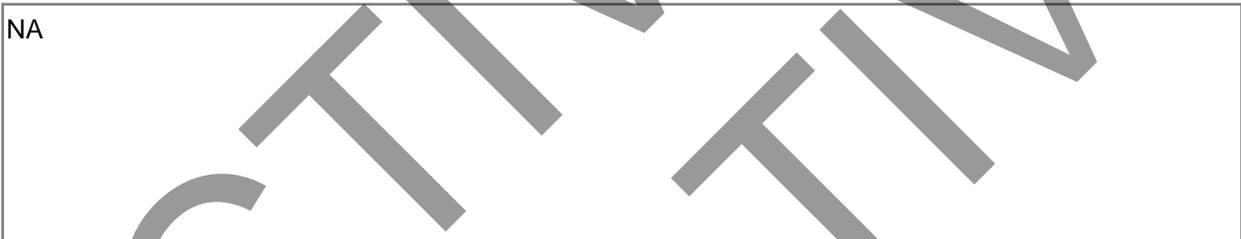
8 Privacy and Security Safeguards

46. Describe administrative safeguards (i.e. policy documents, procedures, or training).

A large black rectangular redaction box covering the entire answer area for question 46.

47. Describe physical safeguards (i.e. locked, filing cabinets, locked doors, or restricted areas).

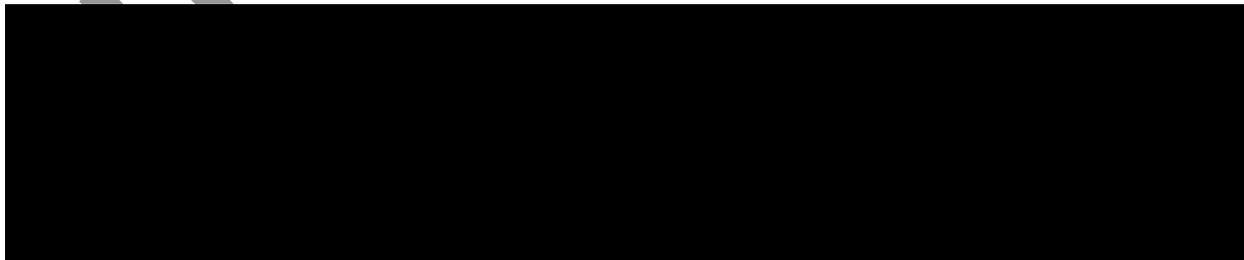
NA

A large black rectangular redaction box covering the entire answer area for question 47.

48. Describe the controls in place to prevent unauthorized access to personal information (i.e. role-based access to software, access logs).

A large black rectangular redaction box covering the entire answer area for question 48.

49. Describe technical safeguards (i.e. firewalls, encryption, or intrusion prevention systems).

A large black rectangular redaction box covering the entire answer area for question 49.

9 Privacy Risk Identification and Mitigation

50. Identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented ([see risk classification table](#)).

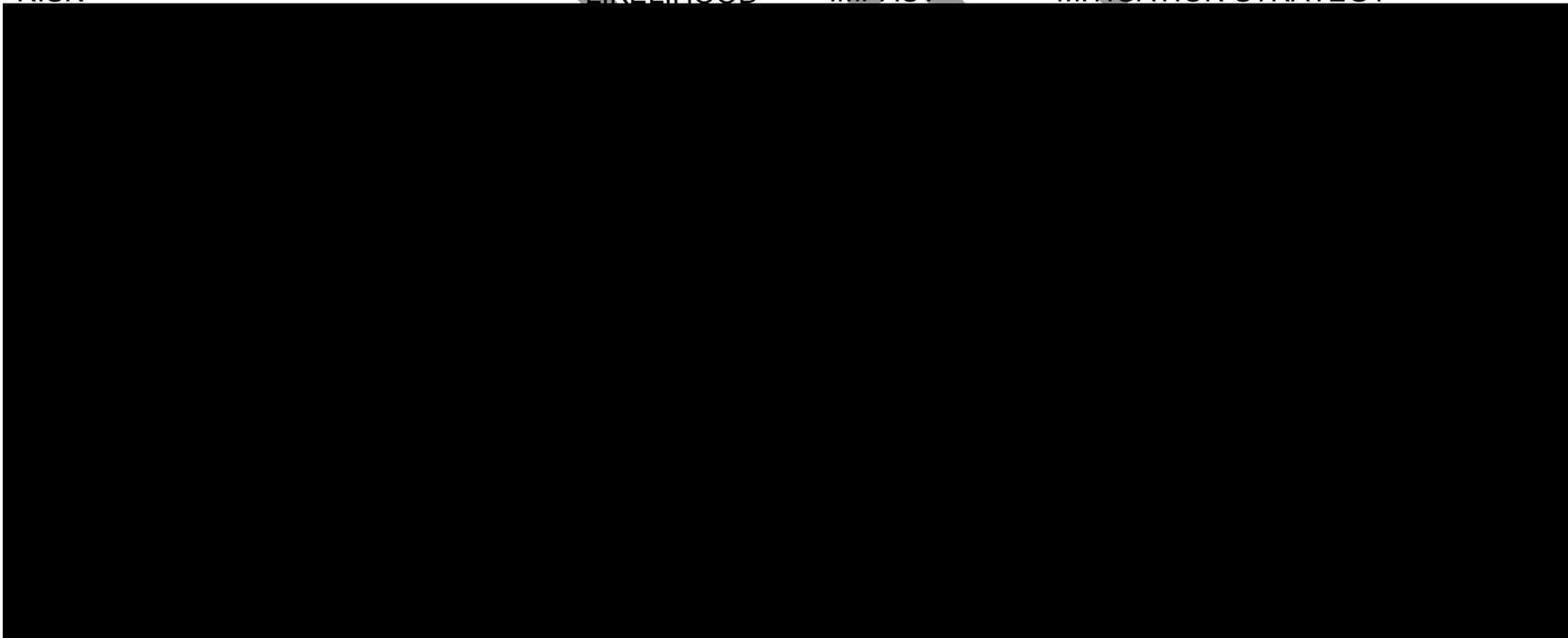
Try to include at least one risk related to each step in the information cycle (collection, storage, access, disclosure, and destruction). **If you are disclosing or storing data outside of Canada you will need to identify additional risks related to storage/disclosure outside of Canada**

RISK

LIKELIHOOD

IMPACT

MITIGATION STRATEGY



RISK

LIKELIHOOD

Low

Moderate

High

IMPACT

Low

Moderate

High

MITIGATION STRATEGY

Low

Moderate

High

10 Data Linking

In FOIPPA, “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.

51. Does this initiative involve a program or activity that provides a service(s) through a public body and at least one other public body or agency working collaboratively to provide that service?

Yes

No

52. Does this initiative involve a program or activity that provides a service(s) through a public body that is working on behalf of one or more other public bodies or agencies?

Yes

No

53. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the Regulations? (Privacy Officer will answer).

Yes

No

If this PIA addresses a common or integrated PIA program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice, and timelines.

11 Conclusions and Approvals

Individual leading the Program/Project: Loralyn Murdoch

Position: Director of Athletics

I confirm the information management practices in this initiative have been documented as accurately as I am aware. I commit to communicating appropriate information management practices to all individuals participating in this initiative. I commit to following the documented practices on this PIA, or arranging a PIA amendment if I am aware information management practices in this initiative change.

July 4, 2023

Signature: _____ Date: _____

Director/Dean Overseeing the Program/Project: Loralyn Murdoch

I am accountable for overseeing my staff involved in this initiative to ensure they adhere to information management practices presented in this PIA. I will arrange for the project lead named above to contact the Privacy Officer to arrange a PIA amendment if required.

Signature: _____ Date: July 4, 2023

Name of Vice-President Kellie Howitt (Senior Governance Officer)

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that complies with policies and procedures of the University of Northern British Columbia.

Signature: _____ Date: November 3, 2023

Name of Privacy Officer: Christopher Ross

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that comply with British Columbia's Freedom of Information and Protection of Privacy Act.

Signature: _____ Date: November 8, 2023

12 Privacy Notice

All collection notices must include the:

- Purpose for the collection
- Legal authority for the collection
- Contact information for an employee of UNBC who can answer the individual's questions about the collection.

The employee should be able to explain why the personal information is being collected and how it will be used, retained, and disclosed.

The contact method should suit the collection method. For example, if you collect personal information through an online form, you could include an email contact.

You can use this template to write your draft collection notice:

Your personal information will be collected for [purpose]. If you have any questions about the collection of this personal information, please contact: name@unbc.ca.

This information is being collected by UNBC under FOIPPA 26(*).

13 Key Terms

“**personal information**” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they relate to another individual,
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Risk Classification Table

*Risk Levels	Likelihood	Harm
Low	Little possibility that the risk will occur due to mitigating factors	Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation.
Moderate	A possibility that the risk will occur if no additional measures are taken.	Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation.
High	Near certainty that the risk will occur in the future if no corrective measures are taken.	Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation.