Procedures Title:	**Privacy Breach Procedures**
Associated Policy:	IT 11.0 Information Access and Privacy Protection
Procedure Holder:	University Secretariat
Executive Lead:	University Secretary and General Counsel
Original Date:	March 2025
Last Revised:	n/a
Next Review:	March 2027

1. Purpose and Background

It is the requirement of the Yukon's Access to Information and Protection of Privacy Act (ATIPP Act) that Yukon University, being a public body, implemented security measures designed to prevent privacy breaches in respect of the Personal Information that they hold.

These Procedures apply to Yukon University employees and, as well as contracted service providers and are established in accordance with the provisions and definitions of the ATIPP Act for public bodies.

The President, as the head of the public body (Yukon University), pursuant to section 30 of the ATIPP Act, is responsible for protection of Personal Information held by Yukon University by securely managing the Personal Information in accordance with the ATIPP Act regulations.

2. Guiding Principles

A Privacy Breach occurs when Personal Information is accidentally lost or altered, or when it is accessed, collected, used, disclosed, or disposed of in an unauthorized manner.

Limiting collection, use, and disclosure of Personal Information minimizes the risk of a Privacy Breach. A person commits an offence if they knowingly fail to secure Personal Information against Privacy Breach.

Any suspected unauthorized collection, use, or disclosure of Personal Information held by Yukon University must be immediately reported to the designated Yukon University Privacy Officer ("Privacy Officer"), in accordance with these Procedures. The Privacy officer will

assess the information, investigate whether the breach has occurred and if it did, make timely and necessary efforts to mitigate it. The Privacy Officer will follow up on any legitimate breach with an assessment report.

3. Definitions

- **Affected Individual**: means an individual whose Personal Information is personal information in respect of which a Privacy Breach has occurred or is occurring. (s. 32(1) of the ATIPP Act, SY 2018, c. 9)
- **Personal Information:** means recorded information about an identifiable individual as provided in the Appendix A below; some exceptions apply and are also provided in the Appendix A below.
- **Privacy Breach**: in respect of Personal Information, means the theft or loss of, or unauthorized use, disclosure or disposal of, the Personal Information. (s. 1 of the ATIPP Act, SY 2018, c. 9)
- **Significant Harm:** in respect of a Privacy Breach, bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property, or any other similar type of harm. (s. 1 of the ATIPP Act, SY 2018, c. 9)

4. Procedures

DISCLOSURE

4.1. If a Yukon University employee reasonably believes that a Privacy Breach has occurred or is occurring, they must immediately report this to the Privacy Officer at privacy.officer@yukonu.ca. The *Privacy Breach Report Form* provided in the Addendum to these Procedures.

ASSESSMENT

4.2. Immediately upon receiving a report, the Privacy Officer

a. must assess it and, if necessary, request any information from any Yukon University department or employee that they consider necessary to conduct

their assessment; the requested information must be provided to the Privacy Officer without delay;

b. make all reasonable and necessary efforts to prevent further spread of the Personal Information (e.g., disabling systems) and to recover the Personal Information or, if recovery is not possible, to ensure the sources who have received it destroy the information (request written confirmation that it is destroyed and no copies retained); and
c. notify the police if the breach involves theft or any other suspected criminal activity.

4.3. If, based on the assessment, a Privacy Breach has occurred or is occurring, the Privacy Officer must, without delay, determine whether there is a Risk of Significant Harm to Affected Individual(s) due to the Privacy Breach, based on the following factors (s. 32(6) of the ATIPP Act, SY 2018, c. 9):

a. the sensitivity of the Personal Information;
b. the probability that the Personal Information is, has been or will be used or disclosed in an unauthorized manner;
c. the time duration between the Privacy Breach occurrence and disclosure;
d. the number of Affected Individuals;
e. the type of relationship, if any, between Affected Individuals and any person who may have used, or to whom may have been disclosed, the Personal Information;
f. the measures, if any, that Yukon University has implemented or is implementing to reduce the risk of Significant Harm to the Affected Individual(s);
g. if the Personal Information has been lost, stolen or disposed of, whether or not any of the Personal Information has been recovered; and
h. any other information that is relevant in the circumstances and is reasonably available to the Privacy Officer.

4.4. Evaluation of Privacy Breaches is contextual. To determine whether there is a risk of significant harm, the Privacy Officer must first determine the Significant Harm associated with the breach in accordance with the factors listed above.

4.5. Keeping the factors in mind, the Privacy Officer must next determine if there is a risk, meaning “possibility” that the individual may suffer or be exposed to the Significant Harm.

4.6. Unless the Privacy Officers is able to conclusively determine through analysis that a risk of harm did *not* occur as a result of a Privacy Breach, then there is a Risk of Significant Harm. If Significant Harm *could* occur as a result of the Privacy Breach, then this is sufficient to assess that a Risk of Significant Harm has occurred.

REMEDIATION

4.7. If the Risk of Significant Harm has been determined (section 4.3 of these procedures), the Privacy Officer must, without delay

a. Notify the President and provide an assessment report (see section 4.3 for guidelines).

b. Notify each Affected Individual and include information required by section 10(7) of the Access to Information and Protection of Privacy Regulations as follows:
   - Date on which it began and a statement that it continues to occur; if it is no longer occurring, the dates/time period during which it occurred, if known.
   - Description and cause of the breach, if known.
   - Description of the types or classes of personal information that are subject to the breach.
   - Description of the risk of Significant Harm to affected individuals, and each measure that the University has implemented or is implementing to reduce it.
   - Business contact information of the University employee who can provide further information related to the breach and risks of Significant Harm.
   - Business contact information of the Commissioner.
   - Text of the following provisions of the ATIPP Act (sections 37 and 90):
     "An individual may, if they reasonably believe that a public body has collected, used or disclosed their personal information in contravention of this Part, make a complaint to the commissioner by filing the complaint in accordance with section 90.
     90 (1) Subject to subsection 106(2), a person who has a right under this Act to make a complaint, and who wishes to have the complaint investigated by the commissioner, must file the complaint
     (a) in the case of an access to information complaint made under section 61 (third party complaint), at least five business days before the response date for the access request to which the complaint relates; or

(b) in the case of any other type of complaint, not later than 30 business days after the day on which the complainant is provided with notice of, or becomes aware of, the decision or matter that is to be the subject of the complaint.

(2) The commissioner may accept a complaint for filing despite the expiry of the time provided for filing of the complaint under paragraph (1)(b), if satisfied that the complainant's inability to file the complaint within the time provided was because of circumstances beyond the control of the complainant."

c. Personal Information not related to the Affected Individual and information that could adversely affect the investigation must not be included.

d. Notification under section 4.7 (b) above, may be given indirectly, through public communication, if it is believed that it will come to the attention of the Affected Individual(s) more quickly and should be following the guidelines provided in the paragraph above. At least one day before providing public notice, the Privacy Officer must give notice to the Commissioner that a public notice will be provided, with the reason and specific means by which the public notice will be provided (section 10(4) of the Access to Information and Protection of Privacy Regulations).

e. Report to the Yukon Information and Privacy Commissioner (" Commissioner") with a copy of the notice to Affected Individuals. The report must include the reasons for determining that a Risk of Significant Harm exists, the assessment of the cause of the Privacy Breach, and measures that Yukon University has implemented or is implementing to reduce the risks for the Affected Individuals.

4.8. The President, within 30 days after the day on which they receive a recommendation from the Commissioner (section 4.4 (c)), must decide whether to implement the measure(s) and provide a notice of their decision on each measure to the Commissioner. Failure to provide notice will be considered as a President's decision to not implement the recommended measure(s).

4.9. After examining the circumstances of the Privacy Breach, remedial actions that the Privacy Officer may need to take include but are not limited to evaluation and revision of institutional policies and procedures, changes to systems and programs involving Personal Information, providing training to staff regarding Personal Information protection and their privacy obligations.

REPORTING

4.10. The Privacy Officer will prepare an annual Privacy Breach report and include the following information as set out in section 42(2) of the PIDWA:

1. The number of disclosures and complaints of reprisal received, and the number acted on and not acted on.
2. The number of investigations commenced; and
3. In the case of an investigation that resulted in a finding of wrongdoing, a description of the wrongdoing and any corrective actions taken or the reasons why no corrective action was taken.
4. In the case of an investigation that resulted in a finding that a reprisal was taken, a description of the reprisal and any corrective action taken or the reasons why no corrective action was taken.

5. Exceptions to the Procedures

There are no foreseen exceptions to these procedures.

6. Problem Solving

Any questions arising out of the content or communication of this policy or disputes arising from a decision made as a result of applying this policy should be first reported to the Executive Lead, who will endeavor to find a resolution with all stakeholders. Failing such a resolution, the matter should be reported to the University Secretariat.

7. Document History

Include all updates here, including non-substantive changes, beginning with formal approval.

Date (Month DD, YYYY)	*Update (*Approver: change)
March 18, 2025	Procedures established under Policy IT 11.0

APPENDIX A

1. **Personal Information**, in accordance with the definition of the ATIPP Act, section 1, means recorded information about an identifiable individual and **includes**:

    (a) their name (*unless it is used for the person's business contact information*)
    (b) their home, mailing or email address or phone number,
    (c) their age, sex, gender identity or expression, or sexual orientation,
    (d) their skin colour, fingerprints, blood type or any other genetic characteristic or biometric information,
    (e) their race, ethnicity or nationality,
    (f) information about their current and past physical or mental health, including their personal health information,
    (g) information about their marital, family, education or employment status or history,
    (h) information about their current or past
        - political or religious beliefs, associations or activities,
        - amounts or sources of income, or
        - income tax returns,
    (i) information about
        - an asset that they wholly or partially own or owned,
        - a liability for which they are or were wholly or partially liable,
        - a transaction or banking activity in which they are or were involved,
        - an assessment of credit-worthiness of which they are or were the subject,
        - a discretionary benefit in the nature of income assistance, legal aid or another similar type of benefit that they are receiving or have received, or
        - a law enforcement matter of which they are or were the subject,
    (j) a personal unique identifier that has been assigned to them,
    (k) another individual's opinion or view about them, or
    (l) their opinion or view about something other than their opinion or view about another individual.

2. Not considered the Personal Information, in accordance with section 3 of the ATIPP Act:

    (a) the Business Contact Information of the individual;
    (b) in the case of an individual who is or was a service provider of a public body, or who is or was an employee or agent of the service provider, the terms of the contract between the public body and the service provider, including, as specified in the contract, the individual's name and, if applicable, their position with the service provider.

Business Contact Information means information that makes it possible to contact the individual at their place of business and includes the individual's name, position, title, business phone number and business email address. (s. 1 of the ATIPP Act, SY 2018, c. 9)