Reporting a Suspected Privacy Breach

What is a Privacy Breach?

The *ATIPP Act* defines a privacy breach as the theft or loss of, or unauthorized access, use, disclosure or disposal of personal information (PI).

The most common privacy breaches occur when PI is stolen, lost or mistakenly disclosed. Some examples of privacy breaches are:

- Faxes that go to the wrong phone number;
- Loss of a flash drive/USB stick or hard drive that was not encrypted;
- A system that maintains PI being hacked into;
- Snooping or browsing through information systems; and
- Unauthorized sharing of personal details about someone with others.

Steps for reporting a suspected breach

The ATIPP Act gives employees the responsibility to report suspected privacy breaches. If you suspect a privacy breach has occurred, please take the following steps:

- Take any immediate steps you can to **CONTAIN** the suspected breach. If you are unsure about what to do that would be appropriate to contain the breach, skip this step and contact your Designated Privacy Officer first.

What is containment?

Containment involves activities that can reduce the impact or stop the suspected breach from occurring. Examples of containments actions are:

- Immediately recovering the information and have the individual/s who received the PI confirm – in writing – that no copies of the information were made, the information was not and will not be communicated to anyone, and all copies have been securely destroyed;
- Shutting down the system that was breached; and
- Revoking or changing computer access codes.

- **CONTACT** your Designated Privacy Officer or the ATIPP Office at privacy@yukon.ca if you are not able to reach your Privacy Officer. Do not include details about the suspected breach in any emails.

- **COMPLETE** the Privacy Breach Reporting Form for Employees and provide it to your Designated Privacy Officer.

Do not take any additional steps outside of immediate containment actions until you receive specific direction from your Designated Privacy Officer or the ATIPP Office.

*** Don't discuss the suspected breach with anyone else***

What happens next?

ASSESSMENT: Your Designated Privacy Officer will work with you to confirm whether a breach has occurred. You may be asked to provide more information.

NOTICE TO AFFECTED PARTIES: If your Designated Privacy Officer determines a breach occurred, others may be notified of the breach depending on the scope of the breach and determination of risk of harm.

CONTAINMENT & MITIGATION: Depending on the scope of the breach, additional containment measures may be needed. You may be asked by your Designated Privacy Officer for assistance during the process.

The ATIPP Office provides advice and guidance to public bodies and Designated Privacy Officers.

You may contact us at any time during the process for assistance with the breach reporting, assessments, mitigations, and notifications.

More detailed information about the breach reporting process can be found in the Privacy Breach Procedures document on the Access to Information Registry.

For assistance, please contact the ATIPP Office at privacy@yukon.ca.