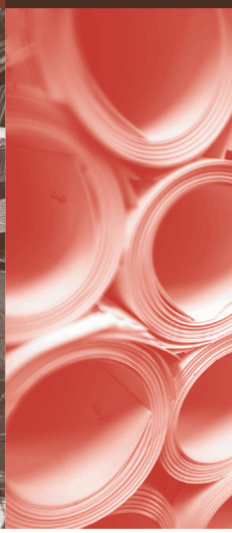
Yukon
Highways and Public Works
enabling yukon



Privacy Breach Reporting Form

1 CONTAINMENT OF BREACH

Name of the Organisation:	
Investigated by:	
Email/Contact:	
Date breach occurred: (YYYY-MM-DD)	
Date breach was discovered: (YYYY-MM-DD)	
Location of breach:	

1.1 Has there been a breach involving "personal information" or "personal health information"?

A "breach" means the accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal of either personal information or personal health information.

Some examples of situations where a breach occurred are:

- *An employee misplaces or loses a USB or laptop;*
- *A computer system is hacked into; or*
- *Information is sent to the wrong person in error.*

Refer to Appendix A for examples of "personal information" and "personal health information".

Example: Bill lost a USB that contained the employee information of ten individuals. The employee information included the following information for each individual: name, date-of-birth, residential address, personal phone number, employee number, employment history and performance evaluations.

Answer:

If you determined a breach has occurred, list the types of information involved (refer to Appendix A).

1.2 List the immediate containment actions.

Some examples of containments actions are:

- *Immediately recovering the information and have recipient confirm – in writing – that no copies of the information were made, the information was not and will not be communicated, and all copies have been securely destroyed;*
- *Shutting down the system that was breached;*
- *Revoking or changing computer access code; or*
- *Contacting your privacy officer.*

Example: When Bill realised the USB was missing, he took the following steps: he immediately contacted his privacy officer and tried to locate the lost USB. Bill retraced his steps; he searched his office and his car. He then contacted the government office where he brought the USB. To Bill's relief, his colleague confirmed he was in possession of the USB.

Next, Bill immediately retrieved the USB from his colleague. Unfortunately, Bill's colleague confirmed he had accessed the contents of the USB. Bill then had his colleague confirm, in writing, that no copies of the USB were

made and the information he viewed will not be communicated.
Answer:

CONTACT YOUR PRIVACY OFFICER BEFORE PROCEDING TO THE FOLLOWING SECTIONS OF THE REPORT

2 RISK OF HARM ANALYSIS

Note: Your privacy officer or delegate should complete the following section.

2.1 What is the cause and extent of the breach?

Include the following when answering: • *What is the cause of the breach?* • *Is there a risk of ongoing or further exposure of the information or has it been contained?* • *Was the information lost or stolen?* • *Is the information encrypted?* • *Is there a suspicion of malicious intent behind the breach?* • *How much information (# of documents or amount of data) was involved in the breach?* ***Example: Bill, along with his privacy officer, determined the breach was caused by the loss of an unencrypted USB stick. Because the USB was recovered within hours of Bill misplacing the USB stick, it was determined there was no risk of further exposure of the information.***
Answer:

2.2 How many individuals are affected?

Consider the following when responding: • *Very few (less than 10)* • *Identified and limited group (>10 and <50)* • *Large number of individuals affected (>50)* • *Numbers are not known* ***Example: Bill determined that an identified and limited group of ten individuals are affected.***
Answer:

2.3 What is the sensitivity of the information and what type(s) of harm could occur?

Part 1- Determine the Sensitivity of the Information

Commissioners have held the following types of information to be highly sensitive: SIN, date-of-birth, driver's license number, credit card numbers, signatures, medical information (psychiatric or addition counselling notes, for example), employee information (poor performance or termination information, for example).

Commissioners have held the following types of information to be low or moderately sensitive: Names, phone numbers, email addresses, and bank accounts.

Part 2 – Determine Harm

Harm to the individual:

Risk of identity theft or fraud: Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, a combination of name, date-of-birth and address, etc…

Risk of physical harm: When the information places the individual at risk of physical harm from stalking or harassment.

Risk of hurt, humiliation, and damage to reputation: Often associated with the loss of information such as mental health records, medical records, criminal history or disciplinary records.

Loss of business or employment opportunities: Where the breach could affect the business reputation of an individual.

Harm to the organisation:

Risk to organisation: Where the organization is concerned that the breach will undermine trust of citizens, loss of assets, financial exposure or contractual and/or legal obligations.

Example: Bill determined that the lost information included highly sensitive information. It included employee information, including personnel evaluations, as well as the name, date-of-birth, and address of individuals.

Next, because the information included employee information, Bill determined that there is a risk of humiliation and damage to the reputation of the affected individuals. Bill also determined there is a risk of identity theft as individuals' name, date-of-birth, and address were included together. Further, Bill determined there is a risk to the organisation as employee trust could be undermined around how the organisation handles their employee information.

Answer:

2.4 Is there a risk of significant harm?

Consider all of the following:

- *The length of time between the breach and its discovery;*

• *The likelihood that there was been any disclosure, unauthorized use or copying of the information;* • *The information available regarding the individual's circumstances;* • *The likelihood that the information could be used for identity theft or fraud;* • *The number of individuals whose information is or may be similarly affected;* • *The relationship between the affected individuals and any individuals who has accessed the information. (This is a factor in a small jurisdiction such as the Yukon.); and* • *The immediate containment measures taken.* ***Example: Bill determined that there was a low risk of significant harm. Bill immediately noticed the USB stick was missing upon returning to his office and promptly located it. Further, Bill received written confirmation that the USB stick was not copied or communicated. Finally, Bill confirmed that his colleague did not know any of the individuals' information he accessed.*** ***As a result, Bill is not required to notify the affected individuals, nor the Office of the Information and Privacy Commissioner.***
Answer:

Note: If you determine there is a risk of significant harm, you must notify the affected individuals as well as the Office of the Information and Privacy Commissioner.

3 NOTIFICATION

3.1 Internal Notifications:

Has the Director of the affected program area been notified?	
Has the Assistant Deputy Minister of the affected program been notified?	
Has the Deputy Minister been notified?	
Has Legal Services Branch of the Department of Justice been notified?	
Have the police been notified, if necessary?	

3.2 Will affected individuals be notified? If not, why not?

Note: If there is a risk of significant harm you must notify the affected individuals, while at the same time give the commissioner a copy of the notice.

When notifying affected individuals, your notice must include:

- *A description of the circumstances of the breach and the information involved;*
- *Indicate when the breach occurred;*
- *Describe the measures, if any, that has been taken to reduce the risk of harm to the individual as a result of the breach, including steps the individual can take; and*
- *Identify who can be contacted within your organisation with questions.*
- *Notify individuals of their right to complain to the Office of the Information and Privacy Commissioner.*

Example: Despite there not being a likelihood of significant harm, Bill determined that he would notify the affected employees as he felt it was the right thing to do. Affected individuals were notified directly, by letter. The letter detailed what happened, the types of personal information involved, when the breach happened, measures taken to prevent similar breaches, and a contact number for any questions.

Answer:

4 PREVENTION

4.1 Describe the physical security safeguards in place.

For example: locked cabinets, securely stored laptops, key card access to the building is used, etc...

Answer:

4.2 Describe the technical security safeguards in place.

For example: use of YG firewall, document encryption, user access profiles assigned and removed on a need-to-know basis, etc...

Answer:

4.3 Describe the administrative security safeguards in place.

For example: what security policies will be used to ensure the personal information is protected; what training or procedures in place so users are aware of access rules.

Answer:

4.4 **What internal improvements to processes, systems, policies, and any other actions to mitigate recurrence are recommended? What is the timeline for implementation?**

The recommended solutions should address any necessary improvements needed to physical, technical and administrative safeguards to reduce future breaches.
Answer:

4.5 **If it was determined there was a risk of significant harm, has the Director, Corporate Information Management (HPW) been forwarded a copy of the completed privacy breach reporting form?**

APPENDIX A: PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION LISTING

Note: This is not an exhaustive list of personal information and/or personal health information.

General PI
name
address
phone number
email address
date of birth
age
gender
criminal record, status or history
anyone else's opinions about the individual
the individual's views or opinions
religious beliefs or associations
country of origin
ethnic or racial origin
political beliefs or associations
marital status
family information or status
visually recorded information (e.g. photo or video of an individual)
educational information (status or history)
employment information (status or history)

fingerprint

type of service received

other

Unique Identifiers

Social Insurance Number (SIN)

Driver's Licence Number

YHCIP# (or other health care number)

other

Personal Financial Information

credit card number

bank account number

income tax information

financial status or history

other

Personal Health Information

YHCIP# (or other health care number)

health care status or history

test results, medical images

medications

diagnosis

disability

other