Privacy Breach Reporting Form

Information Access and Privacy

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the *Access to Information and Protection of Privacy (ATIPP) Act*, 2015 (*ATIPPA, 2015).* Please review the University's Procedure for Managing a Privacy Beach: https://www.mun.ca/policy/site/procedure.php?id=106

If you are aware of a privacy breach that involves your unit, you must complete this form and submit it to the Information Access and Privacy office. Please forward the completed form via email: IAP@mun.ca.

Do not include information in this form that can identify the individual/s whose information has been breached. The IAP office may contact you for further information or clarification. Pursuant to ss. 64(4) of the *ATIPPA, 2015*, the IAP office will submit this report, once finalized, to the Office of the Information and Privacy Commissioner.

1. Contact Information

Department/Unit:	
Division/Program:	
Name and Title:	
Phone:	
E-mail Address:	
Date of Submission of Reporting Form to IAP Office (Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)	

2. Risk Evaluation

Incident Description:	
Date the breach occurred:	
Date the breach was discovered:	

Describe the breach (provide sufficient detail, including cause).

Location of the breach:	
Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised):	

Type(s) of individuals affected (check all that apply):

Client/Customer/ Patient ☐	**Employee** ☐	**Student** ☐	**Other** (please specify):

Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc.):

3. Personal Information Involved

Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). ***Do <u>not</u> include or send us the identifiable personal information.***

4. Safeguards

Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

Describe the **administrative** safeguards (policies, procedures, etc.) currently in place to protect the personal information in your custody and control:

Describe the **technical** safeguards (e.g. access controls, audit controls, etc.) currently in place to protect the personal information in your custody and control:	
☐	Encryption
☐	Password
☐	Other (please specify):

5. Potential Harm

Identify any harm that may result from the breach (check all that apply):

☐	Identity theft (higher risk if breach involves SIN # or financial information)
☐	Physical harm or harassment (e.g. stalking)
☐	Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
☐	Financial cost
☐	Loss of business or employment opportunities
☐	Breach of contract and/or other legal obligations (e.g. from data loss)
☐	Future breaches (technical failures)
☐	Violation of professional standards or certificate standards
☐	Other (please specify):

6. Mandatory Notification

Has the University Access and Privacy Advisor been notified?

☐	Yes	Date notified:	
☐	No	Date to be notified?	

7. Notification of Affected Individual/s

Will the affected individual/s be notified of the privacy breach?

☐	Yes	How will they be notified and when?	
☐	No	Why have you chosen not to notify?	

8. Other Notifications

Have the following been contacted?

	Senior Administration	
☐	☐	Unit Head
	☐	Senior Administrative Officer
☐	Departmental Communications or MarComm	

Have CEP and/or law enforcement officials been notified?

☐	Yes	Who was notified and when:	
☐	No	Will law enforcement be notified at a later time? ☐ Yes ☐ No	

Have you contacted the Office of General Counsel to discuss contractual and/or other legal obligations?

☐	Yes	Who was notified and when:
☐	No	

Important!

You must contact the University Access and Privacy Advisor in the IAP Office to discuss notification of individuals affected by the privacy breach. Please review the University's Procedure for Managing a Privacy Breach available here: https://www.mun.ca/policy/site/procedure.php?id=106

Notification to affected individuals **must** include the following:
You have a right to complain to the Office of the Office of the Information & Privacy Commissioner:

Office of the Information & Privacy Commissioner
3rd Floor, Sir Brian Dunfield Bldg, 2 Canada Drive
P.O. Box 13004, Station "A"
St. John's, NL A1B 3V8
Tel: (709) 729-6309 Fax: (709) 729-6500
Email: commissioner@oipc.nl.ca

For Internal Use by the IAP Office Only

Received by: _____ Date Received: _____