

Procedure for Managing a Privacy Breach

(From the Privacy Policy and Procedures available at: <http://www.mun.ca/policy/site/view/index.php?Privacy>)

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of Part IV of [ATIPPA](#) or, if applicable, a relevant provision of [PIPEDA](#). An example of a privacy breach would be personal information becoming lost or stolen or personal information being mistakenly emailed to the wrong person.

The recommended privacy breach incident protocol has five steps. Step 1 is the responsibility of the individual or individuals who first become aware of the potential breach. The second through fifth steps are the responsibility of the University Privacy Officer, working in cooperation with other University officials and staff, as necessary.

Step 1: Reporting the Breach

Any employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of the University will immediately inform his or her immediate supervisor, the unit privacy officer and the University Privacy Officer. The supervisor will inform the responsible unit head and will verify the circumstances of the possible breach. As soon as the breach has been confirmed to have or have not occurred, the supervisor will inform both the responsible unit head and the University Privacy Officer. This confirmation will occur within 24 hours of the initial report.

The unit head in consultation with the University Privacy Officer will decide whether or not to notify the respective Vice-President or the President as appropriate, by taking into consideration the seriousness and scope of the breach.

When a breach has been confirmed, the University Privacy Officer will implement the remaining four steps of the breach incident protocol.

Step 2: Containing the Breach

The University Privacy Officer will take the following steps to limit the scope and effect of the breach. These steps will include:

- 1) Work with units to immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, or correcting weaknesses in security, and
- 2) In consultation with University officials, notify the police if the breach involves, or may involve, any criminal activity.

Step 3: Evaluating the Risks Associated with the Breach

To determine what other steps are immediately necessary, the University Privacy Officer, working with other University staff as necessary, will assess the risks associated with the breach. The following factors will be among those considered in assessing the risks:

1) Personal Information Involved

- a) What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.
- b) What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?

2) Cause and Extent of the Breach

- a) What is the cause of the breach?
- b) Is there a risk of ongoing or further exposure of the information?
- c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- d) Is the information encrypted or otherwise not readily accessible?
- e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

- a) How many individuals are affected by the breach?
- b) Who was affected by the breach: employees, students, alumni, retirees, public, contractors, clients, service providers, other individuals/organizations?

4) Foreseeable Harm from the Breach

- a) Is there any relationship between the unauthorized recipients and the data subject?
- b) What harm to the individuals will result from the breach? Harm that may occur includes:
 - i) Security risk (e.g., physical safety)
 - ii) Identity theft or fraud
 - iii) Loss of business or employment opportunities

- iv) Hurt, humiliation, damage to reputation or relationships
- c) What harm could result to the University as a result of the breach? For example:
 - i) Loss of trust in the University
 - ii) Loss of assets
 - iii) Financial exposure
- d) What harm could result to the public as a result of the breach? For example:
 - i) Risk to public health
 - ii) Risk to public safety

Step 4: Notification

Notification can be an important mitigation strategy in the right circumstances. The key consideration overall in deciding whether to notify will be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. The University Privacy Officer will work with the units involved and the appropriate University officials to decide the best approach for notification.

1) Notifying Affected Individuals

Some considerations in determining whether to notify individuals affected by the breach include:

- a) Contractual obligations require notification.
- b) There is a risk of identity theft or fraud (usually because of the type of information lost, such as SIN, banking information, identification numbers).
- c) There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment).
- d) There is a risk of hurt, humiliation or damage to reputation (for example when the information lost includes medical or disciplinary records).

2) When and How to Notify

- a) When: Notification of individuals affected by the breach will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted,

those authorities will assist in determining whether notification will be delayed in order not to impede a criminal investigation.

- b) How: The preferred method of notification is direct - by phone, letter or in person - to affected individuals. Indirect notification - website information, posted notices, media - will generally occur only where direct notification could cause further harm, is prohibitive in cost or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

3) What will be Included in the Notification?

Notifications will include the following pieces of information:

- a) Date of the breach
- b) Description of the breach
- c) Description of the information inappropriately accessed, collected, used or disclosed.
- d) The steps taken to mitigate the harm.
- e) Next steps planned and any long term plans to prevent future breaches.
- f) Steps the individual can take to further mitigate the risk of harm.
- g) Contact information for the University Privacy Officer.

4) Others to Contact

Regardless of what obligations are identified with respect to notifying individuals, notifying the following authorities or organizations will also be considered:

- a) Police: if theft or other crime is suspected.
- b) Insurers or others: if required by contractual obligations.
- c) Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.
- d) Applicable research ethics authority
- e) Office of the Information and Privacy Commissioner: The following factors are relevant in deciding when to report a breach to the OIPC:
 - i) the sensitivity of the personal information;

- ii) whether the disclosed information could be used to commit identity theft;
- iii) whether there is a reasonable chance of harm from the disclosure including non pecuniary losses;
- iv) the number of people affected by the breach; and
- v) whether the information was fully recovered without further disclosure.

Step 5: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, the University Privacy Office will investigate the cause of the breach. If necessary, this will include a security audit of physical, organizational and technological measures. As a result of this evaluation, the University Privacy Officer will assist the responsible unit(s) to put into effect adequate long term safeguards against further breach. Policies will be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. The resulting plan will also include audit recommendations, if appropriate.