Introduction

All Michener staff and faculty are responsible for adhering to Ontario privacy legislation and Michener's Privacy Policy. As a public post-secondary education institution, under the *Freedom of Information and Protection of Privacy Act (FIPPA)*, Michener is obligated to address privacy breaches of personal information**.** This protocol sets out detailed expectations, action items, and decision-making criteria to use when faced with a privacy incident or breach involving personal information. The University Health Network's (UHN) Privacy Office manages and supports Michener's privacy program and breach management protocol.

Personal Information is any recorded information that identifies an individual. Privacy **breaches** occur when personal information is managed in a manner that does not follow the rules set out in FIPPA i.e., any occasion where personal information (PI) is:

- lost or stolen;
- collected, accessed, used, or disclosed without authority;
- disclosed without the individual's consent, in a manner inconsistent with FIPPA or otherwise not permitted by law.

A privacy **incident** is an event where personal information is known to be at risk of being breached, is suspected of being breached, or where a policy or protocol that instructs appropriate data management has not been followed. A privacy incident may not necessarily result in a breach, or impact the individual(s) who the information pertains to, but needs to be investigated nevertheless.

All privacy incidents and breaches must be reported to the UHN Privacy Office.

Process

See Appendix A (below) for action items related to each stage in the incident response process.

Roles & Responsibilities

Michener Staff Member or Faculty will:

1. Identify scope of the incident/breach and try to contain it, if possible.
2. Notify their program/department leadership and the Associate Head of Academic Affairs.

Michener Associate Head of Academic Affairs will:

1. Ensure that the incident/breach is contained.
2. Report the incident/breach to the UHN Privacy Office at privacy@uhn.ca, using the Standard Incident Summary below (Appendix B), as soon as possible.
3. Engage any other relevant departments (e.g., IT).
4. Identify appropriate staff for containment, investigation, remediation, and notification activities.
5. Support staff involved in the incident.
6. Work through tasks in incident checklist (see Appendix A below).
7. Create, execute & verify completion of notification plan and materials (where appropriate and in conjunction with Privacy Office and other departments).

Privacy Office will:

1. Provide guidance in managing containment, mitigation, and remediation.
2. Provide guidance on notification plan and materials.
3. Notify the Information and Privacy Commissioner (IPC) (following Privacy investigation and analysis, and only where necessary.

Appendix A

☒	Action	Date Completed
☐	**Step 1: Identify Scope & Notify Internal Parties**	
☐	**Michener:** identify who needs to be engaged and notify them of the incident/breach. • For all incidents: ☐ Appropriate department management ☐ Relevant departments (Registrar, IT, etc.) ☐ UHN Privacy Office • For incidents involving sensitive information (e.g., student accommodation or counselling notes) or unique personal information (e.g., social insurance number): ☐ IT Director (where applicable) ☐ Academic Chair ☐ UHN Corporate Legal	
☐	**Michener:** will use the Standard Incident Summary template (see Appendix B below) to report the incident/breach to UHN Privacy.	
☐	**Step 2: Contain**	
☐	**Michener:** identify the nature of the breach e.g., unauthorized disclosure.	
☐	b identify what information was involved e.g., data elements.	
☐	**Michener and Privacy:** determine whether Michener can re-gain control of the information involved and/or identify how to reduce further impact of the breach.	
☐	**Michener and Privacy:** identify who accessed, collected, used, or received the information involved. This includes when information has been lost or stolen and we cannot confirm who may have it.	
☐	**Michener and Privacy:** where possible, retrieve information and/or confirm deletion. • Request confirmation that information has not been printed, saved, copied, otherwise stored, or further disclosed. • If destroyed, request written confirmation of destruction. • Request & retain contact information of recipient.	
☐	**Michener:** where applicable, take steps to reduce additional unauthorized access (e.g., change passwords, ID numbers or revoke user access).	
☐	**Step 3: Notify Affected Individuals**	
☐	**Michener:** identify affected individual(s).	
☐	**Michener and Privacy:** determine how individuals will be notified and create notification plan, including script or notification letter.	
☐	**Michener and Privacy:** if notification will occur by letter, Privacy and Michener will save copies of each letter in their files once Michener has prepared the letter(s).	
☐	**Michener:** if notification will occur by letter, Michener will courier/mail the letter(s) to the affected individual(s).	
☐	**Step 4: Investigate & Remediate**	
☐	**Michener:** conduct internal investigation to identify root causes, with Privacy direction and support.	
☐	**Michener and Privacy:** determine whether changes to workflows, policies, procedures, protocols, or tools would help reduce the chance of reoccurrence.	
☐	**Michener and/or Privacy:** if applicable, determine whether staff training is needed and implement to prevent recurrences.	
☐	**Privacy:** where applicable, submit breach report to the IPC and coordinate all aspects of IPC-UHN-Michener communication.	
☐	**Michener:** where applicable, remediate by implementing recommendations and/or changes to prevent reoccurrence or similar incidents/breaches.	

Appendix B - Standard Incident Summary

The following chart should be used to report a breach/incident to the UHN Privacy Office as soon as Michener becomes aware of it. Please submit the report to privacy@uhn.ca.

Information Needed	Description
What happened and when (description, date, time, location)?	
What personal, confidential, sensitive, or other information is involved (e.g., type of document, name, address, email address)?	
Approximately, how many individuals are impacted?	
Does the incident include Michener systems or technology (including email)? If yes, which ones?	
Have any immediate steps been taken to contain the incident?	
Who has been notified and/or engaged to help to contain the incident?	
Is the incident a result of human error or is there a more deliberate risk e.g., intentional unauthorized use of personal information?	
Can anything be done to control or reduce the harm/impact to individuals e.g., recall email or revoke systems access?	