PRIVACY BREACH NOTIFICATION PROCEDURE

PURPOSE

The purpose of this document is to provide instructions to members of the University community on how to respond to a breach of privacy in compliance with the University's Access to Information and Protection of Privacy Policy ("Access and Privacy Policy").

PART A

What is considered a breach of privacy

A privacy breach occurs when personal information (PI) is disclosed in contravention of the *Freedom of Information and Protection of Privacy Act ("FIPPA")*. For example, the personal information may be:

- Lost (e.g. a file containing personal information is misplaced within the University),
- Stolen (e.g. a laptop containing personal information is stolen), or
- Inadvertently disclosed through human error (e.g. a letter addressed to person A which contains personal information is actually mailed to person B).
- Intentionally accessed, used or disclosed, without authority (e.g., an employee looks at the personal information of a friend's child, or family member, for non-work related purposes).

PART B

What to do if a privacy breach is suspected or confirmed

If you suspect that an individual's personal information has been breached, you should immediately:

1. **Contain**
   You should take immediate steps to contain the breach. For example:
   - If Personal Information was inadvertently disclosed to another individual, retrieve the hard copies of the Personal Information that was disclosed, ensure that no copies of the Personal Information have been made or retained by the

individual and obtain the individual's contact information in the event that follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other Personal Information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).

2. **Immediately inform:**
   - Your Unit Head, and
     - The University's Privacy Office, the Manager, Privacy & Records Management, by emailing Privacy@Brocku.ca, and
     - Copying (cc'ing) your Unit Head.

3. **Complete Privacy Breach Report Form**
   To document the breach, aid in the investigation, and corrective action:
   - Complete Steps 1 (Contain) & 2 (Assess the Risks) of the Privacy Breach Report Form.
   - Provide a copy of the Privacy Breach Report Form to your Unit Head, and the Manager, Privacy & Records Management.
   - Manager, Privacy & Records Management to complete Step 3 (Investigation & Corrective Measures) of the Privacy Breach Report Form.

PART C

How the University will respond to a privacy breach

The Privacy Breach Report Form will guide you through the steps to be completed for each suspected privacy breach. Here is a summary of each step within the Privacy Breach Report Form, as follows:

Step:

1. **Contain**
   The Manager, Privacy & Records Management will work with you and your Unit Head to ensure the breach is contained. This involves steps to prevent further compromise.

2. **Assess the Risks**
   You should assess the types of Personal Information involved and the sensitivity of the information breached to determine the appropriate response and notification to affected individuals.

Examine the situation fully and work with the Manager, Privacy & Records Management to ensure that any necessary details of the breach and any corrective actions are documented for later investigation and review.

Assess the cause and extent of the breach, as well as the foreseeable harm from the breach (e.g. identity theft, damage to the individual's or University's reputation).

3. **Notify Affected Individuals**
   Identify those individuals whose privacy was breached and inform the Manager, Privacy & Records Management. The Manager, Privacy & Records Management will determine what form of notification is appropriate, with advice from the University's General Counsel & Associate Vice-President, Legal, Compliance & Privacy. In determining whether to notify individuals, the Manager, Privacy & Records Management will take into consideration the following: a) if the information breached is personal health information, and b) whether the information is subject to the General Data Protection Regulation (GDPR) and a risk to the rights and freedoms of the individual is present.

4. **Investigate and Correct**
   The Manager, Privacy & Records Management will further investigate the cause of the privacy breach, work with the unit concerned to prepare documentation and consider whether to develop a prevention plan. A prevention plan may address such issues as employee training, policy review or development, audit of physical and/or technical security, and a process to ensure that the prevention plan has been fully implemented.

5. **Notification of Cyber Incidents**
   The Manager, Privacy & Records Management will consult with ITS Security, and the Associate Director, Enterprise Risk Management & Insurance, regarding any cyber security privacy breaches and adhere to the University's Information Security Incident Response Plan which outlines the appropriate criteria to initiate the cyber incident communication process.

Decisions on how to respond to a suspected or confirmed privacy breach will be made by the General Counsel & Associate Vice-President, Legal, Compliance & Privacy on a case by case basis,

based on advice from the Manager, Privacy & Records Management. The University will take each situation seriously.

Decisions on how to respond to a suspected or confirmed cyber security event will be made in accordance with the Information Security Incident Response Plan with the support, advice, and involvement of the Privacy Office.

General Counsel, in consultation with the affected unit(s), will determine whether Ontario's Information and Privacy Commissioner (IPC), or Ministry of Government and Consumer Services (regarding Cyber Incidents) should be notified of the breach.

PART D

How the University will respond based on the scale of a privacy breach

The Privacy Office makes the determination as to whether the breach is small-scale or large-scale or complex.

- Small scale: If the breach is small scale or not complex, the Privacy Office will manage the breach as above in the Privacy Breach Notification Procedure.
- Large scale: If the breach is large-scale or complex, the Privacy Office will follow the Privacy Breach Incident Response Plan.

June 13, 2024