Privacy Breach Protocol

This protocol outlines the steps to be followed in the event of a suspected breach of personal information at UNB. It affirms the University's commitment and obligation to protect personal information under the custody and control of the institution.

The objective of the privacy breach protocol is to create a procedure that ensures privacy breaches are quickly contained and investigated, individuals affected are notified when required, and corrective measures are put in place to mitigate further breaches.

Procedure

The following steps are to be taken in the event of a breach. Depending on the nature and severity of the breach some of these steps may happen concurrently or occur in an alternate order.

1. Step 1 – Contain the breach

1.1. Immediately take steps to contain the breach. This may include resetting passwords, changing access codes, retrieving misplaced physical files, recovering any personal information that may have been disclosed to someone in error.

1.2. Determine if the privacy breach would allow unauthorized access to any other personal information and take necessary steps to protect that data. For example, change passwords, or temporarily shut down access to an electronic information system.

1.3. Contact ITS immediately if you believe the security of an electronic system has been compromised.

1.4. Immediately contact Security & Traffic if you believe your personal information was stolen. Examples include theft of electronic device, office broken into, car broken into on campus and laptop stolen, etc.

2. Step 2 – Report the breach internally

2.1. Immediately notify your unit head, immediate supervisor, and the Privacy Coordinator upon discovering a suspected or confirmed privacy breach. The notification should include as much detail as possible including:

- The date the breach occurred.

- The date the breach was discovered.
- The number of the individuals affected.
- How you learned of the breach.
- Details of the breach – was it an unauthorized use of the information, unauthorized access to information, accidental disclosure, etc?
- The type of personal information involved. Include all data elements such as name, ID number, SIN, gender, grades, employment history, health information, etc.
- The cause of the privacy breach or contributing factors (e.g. human error, deliberate act, system intrusion, etc.).
- Corrective steps (if any) that have been taken to contain the breach.

3. Step 3 – Investigate

3.1. The Privacy Coordinator will work with the unit to conduct an internal investigation into the privacy breach. The investigation will review the circumstances surrounding the breach to determine and document relevant facts, and to and ensure immediate requirements of containment are addressed.

4. Step 4 – Evaluate risk

4.1. The Privacy Coordinator will evaluate the privacy breach to assess the risk involved. This will include an evaluation of the nature of the personal information involved, the number of individuals affected, and the risks associated with any unauthorized disclosure (i.e. who received the personal information), unauthorized access (i.e. who may have accessed the personal information without authorization), and improper destruction/disposal.

5. Step 5 - Notification

5.1. The following considerations shall be taken into account in determining whether notification of the affected individual(s) is required: risk of significant harm to the individual(s), legal obligations, and contractual obligations.

5.2. If instructed by the Privacy Coordinator, notify in writing the individuals whose privacy was breached. The Privacy Coordinator will provide a template to use. The notification will describe the extent of the breach, the personal information breached, and the steps taken to contain the breach, both immediate and long-term. The letter will also contain the contact information of an individual at UNB who can answer questions (usually the unit head) along with the contact information for the Ombud NB (Access to Information & Privacy Division) in the event the individual wishes to file a complaint.

5.3. In cases where many individuals are affected, or where personal information breached is highly sensitive, the Privacy Coordinator may inform Communications and may

involve Communications in the notification process.

5.4. If personal information was sent to the wrong individual(s), the unit involved will notify individuals in writing who received personal information without authority, either to recover it or to ensure its confidential destruction. The Privacy Coordinator will provide a template to use. The notification will request that the information either be returned to the University, or the individual who received information in error is required to confirm in writing of secure destruction. In cases of electronic records, confirmation is required that the personal information was deleted from the person's desktop computer, email, server, and any other storage device or media in such a way that it cannot be recorded.

5.5. Depending on the severity of the breach, the Privacy Coordinator may notify University departments, faculties, and units of the breach and ask that an indicator or flag be placed on the files of those individuals whose information has been breached. This is an extra security measure intended to protect students, faculty members, staff and any individual from identity theft or fraud or further privacy breaches.

5.6. In the event the privacy breach poses a risk of significant harm to the affected individual(s), the Privacy Coordinator will report the privacy breach to the Ombud NB (Access to Information & Privacy Division) by completing the Ombud NB's Privacy Breach Report Form.

6. Step 6 – Mitigate and Prevent

6.1. The unit head shall take such further measures or actions within their authority to mitigate or correct the privacy breach as may be appropriate, having regard for the seriousness of the privacy breach and evaluation of the risks in step 4.

6.2. The unit head and Privacy Coordinator shall review the adequacy of existing physical, procedural, and technical safety measures used to protect personal information. If required, the Privacy Coordinator may recommend amendments or improvements to existing protocols to protect personal information and mitigate instances of further privacy breaches.

7. Step 7 – Management Review

7.1. The Privacy Coordinator maintains a Privacy Breach Register of all breaches at UNB. A summary of the breaches, including remedial steps taken, findings, recommendations, and corrective measures is reported to the President's Executive Team on a regular basis throughout the academic year.

8. Questions

Contact the Records Management & Privacy Office at rtippa@unb.ca or 453-4710 with any questions about privacy breaches or this procedure.