Privacy Breach Protocol

GOV-060-005 Freedom of Information and Protection of Privacy Policy
Appendix II

1. Purpose

This protocol affirms the University of Regina's commitment and obligation to protect personal information under the custody and control of the institution.

This protocol requires the immediate reporting of all Breaches and alleged or suspected Breaches to the individual who has been designated as the Head, Freedom of Information and Protection of Privacy (the "**Head**"), and outlines the steps to be followed when a Breach is reported. This protocol's aims are to ensure that Breaches are quickly contained and investigated, individuals impacted by the Breach are notified, and the potential for further unauthorized collection, use or disclosure of personal information is mitigated.

A "**Breach**" is the actual, alleged or suspected unauthorized collection, use or disclosure of personal information.

2. Sources

Privacy Breach Guidelines for Government Institutions and Local Authorities dated August 2022 (Office of the Saskatchewan Information and Privacy Commissioner)

Guide to Creating an Internal Privacy Breach Investigation Report dated September 2020 (Office of the Saskatchewan Information and Privacy Commissioner)

3. Procedure

Step 1 – Notify the Head

If a student, faculty member or staff member becomes aware of or suspects a Breach, they must notify the Head immediately:

David Meldrum
Head, Freedom of Information and Protection of Privacy
(306) 585-5163
privacy.access@uregina.ca

The notification should include the following details:

1. When did the Breach occur?
2. When was the Breach discovered (if different from above)? How did you learn of the breach?
3. Details of the Breach – was it an unauthorized collection, use, accessing or disclosure of personal information?
4. What type of personal information is involved (examples of personal information include individuals' names, student identification numbers, social insurance numbers, credit card / banking information, gender, employment history, grades etc.)?
5. Who was involved in or witnessed the Breach?
6. What caused or contributed to the Breach (human error, deliberate act, system intrusion, etc.)?
7. What corrective steps (if any) have been taken to contain the Breach or as a result of the Breach?

Upon receipt of notification of a Breach the Head will undertake the following steps:

Step 2 - Determine if a Breach has, in fact, occurred.

In some cases, it is not immediately clear whether or not personal information has been accessed and/or compromised. For example, in case of a cyber security incident, it is not immediately clear which files may have been accessed (if any), or whether such files contain personal information. In cases where it is unclear whether or not a Breach has occurred, further investigation will be required.

Step 3 - Contain the Breach

Immediate steps must be taken to ensure that personal information is no longer at risk. These steps may include:

- Secure any records associated with the Breach
- Isolate and suspend access to any system associated with the Breach
- Secure any computers or devices involved in the Breach
- Suspend processes or practices that are believed to have caused or contributed to the Breach
- Any other actions as deemed necessary by the Head or the Response Team

Step 5 - Determine the severity of the Breach.

The severity of the Breach will be assessed depending on the number of individuals that may have been affected, the nature of the personal information improperly collected, used, accessed, disclosed or compromised, and the potential impact of the Breach on the affected individuals.

Step 6 - If applicable, establish a Response Team.

Each Breach is unique and fact / circumstance specific. In cases where the Head deems it appropriate she will establish a group of people (the **"Response Team"**) who will be responsible to oversee the containment, investigation, notification, reporting, and monitoring of, and response to, the Breach. The Response Team will be comprised of:

- The Head
- The Director, Communications and Marketing
- The Associate Vice-President, Information Services (if relevant to the nature of the breach)
- Other individuals as deemed appropriate by the Head, if beneficial to provide specific expertise or information
- External legal counsel may also be engaged as necessary

If the Response Team is established it shall meet as soon as practicable after notification of the Breach to develop an initial containment strategy, investigation plan and notification plan, and to determine whether notification of law enforcement, the office of the Information and Privacy Commissioner (the **"IPC"**), or other entities is warranted.

As deemed appropriate or warranted by the Head or the Response Team the Head will proactively report the Breach to the IPC, and provide updates as requested or required.

After the initial meeting, the Head will advise the University Executive Team (the **"UET"**) of the known circumstances and provide updates as appropriate throughout the process.

Note that for a Breach of lesser severity, the Head may determine that the establishment of a Response Team is unnecessary. In these situations, any references to the responsibilities of the Response Team in this document will instead be the responsibility of the Head.

Step 7 - Investigation of the Breach (the **"Investigation"**)

The Head or the Response Team will commence an investigation in an attempt to establish:

- Confirmation that a Breach occurred
- The source or cause of the Breach
- The nature and sensitivity of the personal information involved
- The number and characteristics (students, faculty/staff, donors, etc.) of individuals affected
- Any other factors relevant to the circumstances

Depending on complexity of the situation, the Response Team may engage the University Internal Auditor and/or external consulting expertise to assist with the Investigation of the Breach.

In cases where an employee or student has intentionally, and without authorization, collected, accessed, used or disclose personal information of other individuals (**"Snooping"**), Human Resources or the Associate Vice-President Student Affairs (in cases of potential non-academic misconduct by students) may also be advised and consulted.

Step 8 – Notify individuals affected by the Breach

Once the Breach has been confirmed, contained and investigated, the University will notify the affected individuals as deemed appropriate by the Head or the Response Team[1]. There may be circumstances where individual contact may not be possible, in which case media advisories or other means of notification may be considered. In determining the appropriate notification plan the University will balance the benefit of notification with the potential harm arising therefrom. In particular, details respecting the cause or source of the Breach may not be made public, if there is a concern for the safety and security of other University or personal information.

Notification of a Breach will typically include the following information:

[1] Pursuant to section 28.1 of the Act, a local authority shall take reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

- A description of the Breach
- A description of the personal information involved
- If appropriate, a description of the steps taken and planned to mitigate the harm and to prevent future breaches
- Advice on actions individuals can take to mitigate the risk of harm and protect themselves
- Contact information for the Head
- A statement that the University is working with the IPC to address the matter (if applicable)
- If advisable in the circumstances, a notice that individuals have a right to contact the IPC, and a statement that the University is working with the IPC to address the matter (if applicable)
- Recognition of the impacts of the Breach on the affected individuals and an apology (as applicable)

Step 8 – Reporting and follow-up

Once the Investigation is complete, a report will be prepared by the Head outlining the results of the Investigation, including any recommendations to mitigate future Breaches (including possible additional or revised training, safeguards, practices, policies and procedures). A copy of the report will be provided to the IPC, if required.

Recommendations will, if possible, include specific timelines and responsibility for implementation of actions. There may be situations where the Head may request that the University Internal Auditor conduct a review to assist in providing advice and recommendations to prevent recurrence of a similar Breach.

Including in cases of employee snooping, disciplinary measures may be taken against the employee(s) involved in the Breach.