**PRIVACY BREACH PROCEDURES**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Advisor/Company Name)

**Contact Information**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Privacy Officer)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Address)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Telephone #)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Fax #)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Email address)

At ***(Company Name),*** we have a responsibility for the safekeeping and protection of personal information that we collect and retain on our employees & clients.

Part of our responsibility is to document and report any privacy violations/breaches of such personal information.

**What is a breach?**

A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information.

**Why you should notify individuals in certain circumstances**

Your customers and employees expect businesses to protect their personal information. They want to be informed about privacy risks associated with your personal information handling practices.

**What to do after discovering a breach**

* **Complete privacy breach incident form**
  + Complete form in full, include all details
* **Conduct preliminary assessment**
  + Contain breach
  + Designate individual to start investigation
  + Preliminary notification
    - Escalate internally (personal responsible for privacy compliance)
* **Evaluate the risks**
  + what personal information was involved
  + what was the cause and extent of the breach
  + how many individuals have been affected and who are they
  + what harm could result from the breach
* **Notify all appropriate parties**
  + Financial Institution
  + Client
  + Police
  + Privacy Commissioner
* **Prevent future breaches**
  + Review and establish new policies/prodigal/training (if applicable) to prevent future breaches

**Privacy Breach Checklist**

(Guidelines & Steps to assist you with reporting)

### Incident Description

* When was the date of the incident?
* Who discovered it?
* Details of what happened?

### Step 1: Breach Containment and Preliminary Assessment

* Have you contained the breach (recovery of information, computer system shut down, locks changed)?
* Have you designated an appropriate individual to lead the initial investigation?
* Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
* Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?

### Step 2: Evaluate the Risks Associated with the Breach

**(i) What personal information was involved?**

* What personal information was involved (name, address, SIN, financial, medical)?
* What form was it in (e.g., paper records, electronic database)?
* What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

**(ii) What was the cause and extent of the breach?**

* Is there a risk of ongoing breaches or further exposure of the information?
* Can the personal information be used for fraudulent or other purposes?
* Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
* Has the personal information been recovered?
* Is this an isolated incident?

**(iii) Who has been affected by the breach (employees, clients, service providers, other organizations)?**

**(iv) Is there any foreseeable harm from the breach?**

* What harm to the individuals could result from the breach (e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?
* Do you know who has received the information and what is the risk of further access, use or disclosure?
* What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)
* What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

### Step 3: Notification

**(i) Should affected individuals be notified?**

* What are the reasonable expectations of the individuals concerned?
* What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
* Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual’s reputation?
* What are the legal and contractual obligations of the organization?
* If you decide that affected individuals do not need to be notified, note your reasons.

**(ii) If affected individuals are to be notified, when and who will notify them?**

* What form of notification will you use (e.g., by phone, letter, email or in person, website, media, etc.)?
* Who will notify the affected individuals? Do you need to involve another party?
* If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

**(iii) What & Who should be included in the notification?**

Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

* a description of the personal information involved in the breach;
* contact information in your organization who can answer questions or provide further information;
* whether your organization has notified a privacy commissioner’s office;
* Should any privacy commissioners’ office be informed?
* Should the police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions, or credit reporting agencies; other internal or external parties such as third-party contractors, internal business units not previously advised of the privacy breach

### Step 4: Prevention of Future Breaches

* What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?

**Privacy Breach Incident/Reporting Form**

|  |  |
| --- | --- |
| Date: |  |
| Name of Individual completing form |  |
| Location & date of incident |  |
| Description of incident |  |
| Cause (if known) |  |
| Effected individual(s) (client, employee, advisor, 3rd party) |  |
| Type(s) of personal information involved |  |
| Brief description of action(s) taken to contain breach |  |
| Who has been notified (including date notified) |  |
| Additional Comments |  |

**Staff - Privacy Training**

**Training sessions and meetings:**

|  |  |  |
| --- | --- | --- |
| **Date** | **Topic** | **Employee Name** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**­­­­­­­­­**

**Privacy Policy Review Log**

|  |  |  |
| --- | --- | --- |
| **Review Date** | **Item updated** | **Reviewer Name and Title** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |