info@privatech.ca
p.905.886.0751

www.privatech.ca

16 Northumberland Terrace
Thornhill ON, L3T 7E5

PRIVATECH

SAMPLE PRIVACY BREACH RESPONSE PROCEDURE

Personal Information: Any information about identifiable individuals, such as customers, applicants, volunteers or employees of ABC Co., regardless of whether or not such information is considered sensitive.

Privacy Breach: Any loss of, unauthorized access to, or unauthorized disclosure of Personal Information that is directly or indirectly caused by ABC Co., whether identified internally or externally. A privacy breach may be a consequence of a faulty organizational procedure, lack of a security safeguard, operational break-down or human error.

Significant Harm: Bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

PROCEDURE SUMMARY STATEMENT

This Procedure has been adopted to allow for prompt and reasonable action by ABC Co. in the event of a Privacy Breach. It will provide guidance on all reasonable steps necessary to limit, to the extent possible, substantial harm or inconvenience to individuals whose Personal Information has been compromised.

ABC Co. shall ensure a consistent, compliant approach to the handling of Privacy Breaches. Each department of ABC Co. is responsible for integrating this Procedure into its operations and incident response programs.

STEPS FOR RESPONDING TO A PRIVACY BREACH

1. Breach Containment and Preliminary Assessment

Immediate common sense steps will be taken to limit the Privacy Breach and its consequences, including:

info@privatech.ca
p.905.886.0751

www.privatech.ca

16 Northumberland Terrace
Thornhill ON, L3T 7E5

- Contain the breach, e.g. put an end to the unauthorized practice, recover the records, shut down the system that was privy to the breach, revoke or change computer access codes or correct weaknesses in physical or electronic security.

- Designate an appropriate individual to lead the initial investigation. This individual should have appropriate authority within ABC Co. to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

- Inform ABC Co.'s Privacy Officer of the breach. Determine who else needs to be made aware of the incident internally.

- Determine the need to assemble a team comprised of representatives from appropriate parts of the business.

- If the breach is deemed to involve theft or other criminal activity, police must be notified.

- Ensure an investigation of the breach is not compromised. Any and all evidence that are potentially valuable in determining the cause of the breach or that would allow ABC Co. to take appropriate corrective action must not be destroyed.

2. Assess Risks Associated with the Privacy Breach

Information about the breach must be collected, followed by an assessment of the level of risk.

(i) Circumstances of the Breach and Personal Information Involved

Gather the following information in order to determine if there has been "Significant Harm":

- Determine what exactly happened, and to the extent possible, the cause of the Privacy Breach.

- Determine whose Personal Information has been compromised by the breach and the type of information compromised.

info@privatech.ca
p.905.886.0751

www.privatech.ca

16 Northumberland Terrace
Thornhill ON, L3T 7E5

- Determine the number of individuals affected by the breach.

- Were a number of pieces of Personal Information breached, thus raising the risk of misuse?

- Identify the level of sensitivity of Personal Information compromised. Some information is considered more sensitive than others, e.g. health information, social insurance numbers, driver's licenses, health care numbers, credit or debit card numbers. The greater the level of sensitivity, the greater the risk of harm to individuals. Note however that the circumstances of the breach may make the information more or less sensitive.

(ii) Probability of Misuse

Answer the following questions in order to identify "Real Risk":

- How likely is it that someone would be harmed by the breach?

- Who actually accessed or could have accessed the Personal Information?

- How long has the Personal Information been exposed?

- Is there evidence of malicious intent (e.g., theft, hacking)?

- Is the breached information in the hands of an individual/entity that represents a reputation risk to the individual(s) in and of itself? (E.g. an ex-spouse or a boss depending on specific circumstances).

- Was the information exposed to limited/known entities who have committed to destroy and not disclose the data?

- Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm? (E.g. in the case of an accidental disclosure to unintended recipients).

- Was the information exposed to individuals/entities who are unknown, or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?

- Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it? (E.g. information thieves).

info@privatech.ca
p.905.886.0751

www.privatech.ca

16 Northumberland Terrace
Thornhill ON, L3T 7E5

PRIVATECH

*** END OF SAMPLE ***

Complete sample policy + breach response form is 10 pages in length. Other topics covered in this policy include:

- Breach escalation and review
- Individual notification (procedure to notify, content of notification, others to contact)
- Data breach recordkeeping
- Prevention of future breaches
- Complete privacy breach response form for submission to the Privacy Officer

Purchase complete policy (in Word format) at:
https://privatech.ca/privacy-resources/the-privacy-documentation-suite/