NATIONAL PRIVACY COMMISSION

The NPC is an attached agency of the Department of Information and Communications Technology

Data Breach Prevention

The cost of data breaches continues to rise. In 2016, an IBM and Ponemon Institute study found that the average cost of a data breach now stands at $4 million. Thus, a data breach prevention strategy has never been more important.

What is a security incident management policy?

It refers to policies and procedures implemented by a Personal Information Controller or Personal Information Processor to govern the actions to be taken in case of a security incident or personal data breach

They ensure, among others, the following:

1. The creation of a data breach response team

2. The implementation of organizational, physical and technical security measures and personal data privacy policies

3. The implementation of an incident response procedure

4. The mitigation of possible harm and negative consequences of a personal data breach

5. The compliance with the Data Privacy Act, its IRR and other related issuances by the National Privacy Commission.

What must a data breach response policy contain?

1. Protocol for immediate discovery of security incident, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents

2. Reporting plan for incident discovery, including the identification of person or persons responsible for incident response procedure, as well as a contact person in the event of a possible or confirmed Personal Data Breach

3. Procedure for the conduct of preliminary assessment, including:
   - Nature and scope of the breach
   - Impact of breach and immediate damage to data subjects
   - Need for notification of law enforcement or external expertise
   - Immediate security of evidence
   - Measures to contain the security incident and restore integrity to the system

4. Evaluation method for security incidents or personal data breaches that determine:
   - nature, extent and cause of breach
   - adequacy of safeguards in place
   - immediate and long-term damage
   - impact of the breach and potential harm and negative consequences to affected data subjects

5. Coordination plan with law enforcement if the breach involves possible criminal violations

6. Policies and procedures for full-blown and extensive investigation

7. Notification procedure for the National Privacy Commission and data subjects

8. Mitigation measures for possible harm and negative consequences in the event of a personal data breach, including immediate assistance to affected data subjects.

How can one minimize the risk of security incidents or personal data breaches?

- Create a data breach response team where each member has a specific role.
- Implement measures and policies that prevent or minimize security incidents.
- Designate a data protection officer.
- Conduct a privacy impact assessment.
- Train personnel to identify, assess, mitigate and report security incidents or personal data breaches.
- Regularly monitor for security breaches and scan the vulnerability of computer networks.
- Identify data sources, inventory sensitive data, and map locations.
- Draft an incident response policy to contain security incidents and restore system integrity.
- Plan a mitigation method that will address possible harm and negative consequences on data subjects in the event of a breach.
- Ensure compliance with the Data Privacy Act, its IRR and other issuances by the National Privacy Commission.
- Conduct a self-audit plan to include data security and compliance assessments.
- Regularly review and update policies, procedures, and other measures applicable to the system.
- Formulate a data retention and data destruction policy.
- Regularly update back-up or restoration systems for reference and comparison of personal data.