The Annual Security Incident Report

Francis Euston R. Acero
Complaints and Investigations Division

NATIONAL PRIVACY COMMISSION

Definitions

Get everybody on the same page

NATIONAL
PRIVACY
COMMISSION

Event

An observable occurrence in an information system that actually happened at some point in time. (SANS)

NATIONAL
PRIVACY
COMMISSION

Incident

An adverse event in an information system, which includes the threat of an adverse event (SANS)

NATIONAL
PRIVACY
COMMISSION

Security Incident

An event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place. (Sec. 3.J, NPC Circular No. 16-03)

NATIONAL
PRIVACY
COMMISSION

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. (Section 3.F, NPC Circular No. 16-03)

NATIONAL PRIVACY COMMISSION

Nature of Personal Data Breach

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;

2. Integrity breach resulting from alteration of personal data; and/or

3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

NATIONAL PRIVACY COMMISSION

The Annual Report

Contents
Documentation
Deadline for Submissions

NATIONAL
PRIVACY
COMMISSION

What's in the annual report?

- Summary of Data Breach Reports
- Aggregate Security Incidents (Not Resulting in a Breach)
  - Indicate number of incidents and breaches encountered
  - Classified according to impact on availability, integrity and confidentiality

NATIONAL PRIVACY COMMISSION

Active Documentation

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements.

Any or all reports shall be made available when requested by the Commission.

NATIONAL
PRIVACY
COMMISSION

Data Breach Report

- The facts surrounding the incident

- The effects of such incident

- The remedial action taken

NATIONAL PRIVACY COMMISSION

Aggregated Data

- Security incidents not involving personal data
- General information that must include number of incidents and breaches encountered

NATIONAL PRIVACY COMMISSION

TEMPLATE:
Annual Data Breach Report Summary Page

Breach Type	Total Number of Security Incidents Involving Personal Information	Information Impact Categories			
		None	Privacy Breach	Proprietary Breach	Integrity Loss
Confidentiality	10	1	2	3	4
Integrity	6	0	1	2	3
Availability	3	0	0	1	2

Information Impact Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table C

Breach Type	Definition
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27000:2016 Section 2.12)
Integrity	Property of accuracy and completeness (ISO/IEC 27000:2016 Section 2.40)
Availability	Property of being accessible and usable upon demand by an authorized entity (ISO/IEC 27000:2016 Section 2.9)

Information Impact Categories

| Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Proprietary Breach	Unclassified proprietary information was exfiltrated or compromised
Privacy Breach	Personal data was exfiltrated
Integrity Loss	Personal data was changed or deleted

NATIONAL PRIVACY COMMISSION

Template

Annual Security Incident Report
Data Breach Information
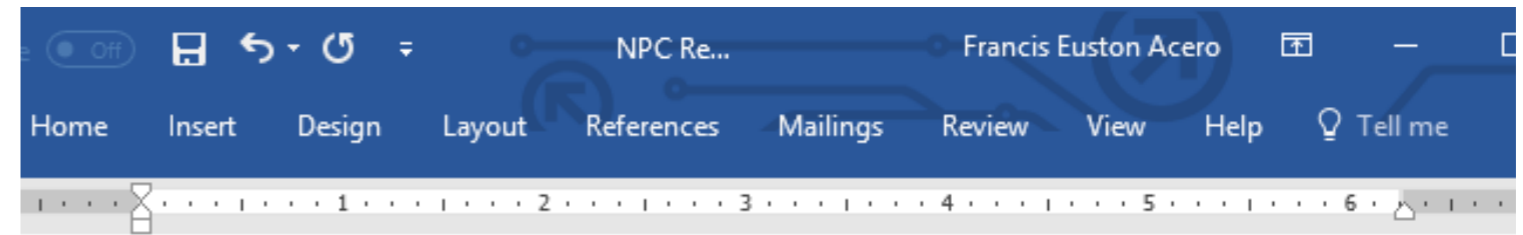
TEMPLATE:
Annual Security Incident Report (Data Breach Information)

Personal Data Breach No. 1
NPC Registration of Data Processing Systems
December 25, 2017

Facts
On December 25, 2017, the MIS failed to renew our SSL Certificate registration.
That same day, despite the failure to renew SSL Certificate registration, data was entered into the Registration of Date Processing System database through unencrypted sessions.

That same day, the MIS informed the DPO that attackers were able to access data entered in the unencrypted sessions.

On December 26, 2017, the DPO shut down all processing related to the Registration of Data Processing Systems.

Effects/Consequences
The absence of a valid SSL Certificate led to unencrypted sessions, which the attackers got authentication cookies and altered data.

The stolen sessions and credentials affected integrity of the database of the Registration of the Data Processing System

Remedies/Action Taken
On December 26, 2017, the MIS chief, on instruction of the DPO, led the response, which was to install a valid SSL Certificate.

From December 26 to 31, 2017, the CMD, acting under instruction of the DPO, restored integrity to the Registration of the Data Processing System data process.

3403 words

NATIONAL PRIVACY COMMISSION

Submissions

Digitally signed submissions are acceptable.

Notarization not required

E-mail
reports@privacy.gov.ph

Registered Mail
3rd Floor, Core G
GSIS Complex
J.W. Diokno Blvd.
Pasay City

5th Floor, PICC
Vicente Sotto St.
Pasay City

Questions?

https://privacy.gov.ph
facebook.com/privacy.gov.ph
twitter.com/privacyph

NATIONAL
PRIVACY
COMMISSION