FORM 1
UNIVERSITY OF THE PHILIPPINES
INITIAL SECURITY INCIDENT OR DATA BREACH NOTICE FORM

The efficient and effective management of security incidents[1] and data breaches[2] involving personal data (personal and sensitive personal information) is required in order to ensure that University of the Philippines System Administration Offices are able to comply with the Philippine Data Privacy Act of 2012, maintain the confidentiality, integrity and security of our processing systems and the data we hold, and ensure mitigating and remedial measures can be put in place promptly so that the rights of data subjects are protected and upheld.

Pursuant to UP's Acceptable Use Policy, this form can be accomplished by any member of the UP community who becomes, or is made aware of a security incident or personal data breach. A non member of the UP community may likewise use this form in order to report an incident or breach e.g. a research participant whose data is involved in an incident or breach. Since time is of the essence, a report may be made via a call to the concerned offices e.g. UP ITDC or the office whose data processing system may have been involved in the incident or breach. It is the authorised personnel of such offices who may fill up the form based on information provided through such call.

This form should be completed (if practicable) as soon as possible and submitted without undue delay to the email addresses below. **In the case of personnel of the unit or office whose data processing system is involved in the incident or breach s/he must submit the report within two (2) hours from knowledge or awareness of such an incident or breach.** This form must be emailed to the head of the office whose data processing system was affected by the incident or breach (email addresses and office numbers of UP System offices are available at https://up.edu.ph/up-system-officials-and-offices/),the UP ITDC CERT@up.edu.ph, the Office of the President op@up.edu.ph and the UP System Data Protection Officer dpo@up.edu.ph. The contact information of Constituent University officials and offices is available through the CU

[1] *Security incident* is 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.

[2] *Personal data breach* refers to 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. A personal data breach may be in the nature of:

(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.

websites. A person reporting such incident or breach is also requested to call the concerned offices to report such incident or breach and thereafter to provide a hard copy of the report to the concerned offices for documentation purposes as well as in cases when UP IT systems are down e.g. UP mail, MS Office email or homegrown CU email services are unavailable. VOIP numbers of UP System offices are available at https://voip.up.edu.ph/. Landline office numbers of UP System offices are available at https://up.edu.ph/up-system-officials-and-offices/. The UP Office of the President and UP System Data Protection Officer may be contacted via telephone numbers (632) 89280110. The UP ITDC Director may be contacted through telephone numbers 8920-2080 / (632) 8981-8500 local 4469.

As stated above, UP ITDC or other UP personnel may also fill up this form on behalf of a person reporting an incident or breach through a phone call.

Please treat the information contained within this form as strictly confidential. It is UP, through its authorised offices or officials that will inform the affected data subjects as well as the NPC pursuant to the DPA.

I.REPORTING PERSON DETAILS:

Name:

Unit/Office:

Telephone number:

Cellphone number:

Email address:

Your above personal information will be processed by UP for the purpose of efficiently communicating with you regarding the incident or breach and for such other related purposes as allowed by the DPA e.g. providing the relevant information to UP offices tasked with handling the incident or breach as well as law enforcement if necessary.

NOTE: If the above information was filled up by UP ITDC or personnel of other offices in behalf of a person reporting through a call please fill up the following:

Name of UP ITDC or other office staff receiving the report via call:

Unit/Office:

Telephone number:

Cellphone number:

Email address:

Your above personal information will be processed by UP for the purpose of efficiently communicating with you regarding the incident or breach and for such other related purposes as allowed by the DPA e.g. providing the relevant information to UP offices tasked with handling the incident or breach as well as law enforcement if necessary.

II. SECURITY INCIDENT OR DATA BREACH DETAILS:

Time and Date of Incident (you may provide an approximate time and date, indicate earliest approximate time and date possible as this will help uphold the right of data subjects)

Data Processing System involved

Type of data involved

Please refer to the definitions in the footnotes below and list all information involved under each category

a. Personal information (information that can be used to identify an individual including pseudonymized information or information which when put together with other information will identify an individual excluding sensitive personal information which should be indicated in item b below)

b. Sensitive personal information[3]

c. Other information that may be used to perpetrate identity fraud[4]

[3] *Sensitive personal information* refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

[4] Other information shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification

If you are not certain whether information is personal information kindly indicate such pieces of information below[5]:

Is there reason to believe such information has been acquired by an unauthorized person ? ___ Yes ___No ___ Not Sure (check appropriate answer) Please provide details.

Do you think that UP or the National Privacy Commission will consider such acquisition to be likely to give rise to a real risk of serious harm to any affected data subjects ? ___ Yes ___No ___ Not Sure Please provide details.

Number of data subjects or records involved. Please indicate if you are providing an estimated or approximate number of subjects or records.

Does the incident or breach involve:

(a) Information that will likely affect national security, public safety, public order, or public health ___ Yes ___No ___ Not Sure

(b) At least one hundred (100) individuals ___ Yes ___No ___ Not Sure

(c) Information required by applicable laws or rules to be confidential ___ Yes ___No ___ Not Sure

documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

[5] … genetic data can only be considered personal data if it can directly identify a specific individual. A genetic sample by itself is not personal data unless it is analyzed to produce data which can identify a specific individual.Similarly, anonymized or aggregated genetic data without any identifiers or which can no longer be related to any specific genetic identity or profile shall not be considered personal data. See NPC Advisory Opinion 2021-23
https://www.privacy.gov.ph/wp-content/uploads/2021/07/Redacted-Advisory-Opinion-No.-2021-023.pdf

(d) Personal data of vulnerable groups [6]___ Yes ___No ___ Not Sure e.g. students, patients, vulnerable research participants [7]

Nature of incident or breach (Does the same involve the confidentiality, integrity or availability of data?)

Cause or possible cause of such incident or breach (Examples dedicated denial of service attack, hacking, phishing, spoofing, loss or theft of equipment or storage media)

If loss of theft of equipment or storage media is involved

a. Is equipment self or UP owned?

b. What technical measures, if any, will help prevent unauthorised access e.g. remote wiping[8], cellphone, laptop or PC is password protected

   Are UP files in laptop/PC/storage media e.g. USB, external drive encrypted[9]?

Extent or scope of such incident or breach

[6] Processing operations performed on vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor require special protection. NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043.

[7] There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the Commission to comply.

[8] MC 2016-01, SECTION 21. Remote Disconnection or Deletion. A government agency shall adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency, or the deletion of personal data contained therein, in event such mobile device is lost. A notification system for such loss must also be established.

[9] MC 2016-01 SECTION 26. Portable Media. A government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.

Measures done if any to respond to the incident or breach

Other information that will enable the University authorities concerned to address the threats posed by such incident or breach or to evaluate whether or not to notify data subjects and the NPC.

a. Describe how the security incident or breach occurred and the data processing system vulnerability that allowed such security incident or breach

b. Provide a chronology that describes how the security incident or breach occurred; describe individually the events that led to the loss of control over the personal data.

Recommendations and comments if any