FORM 2
UNIVERSITY OF THE PHILIPPINES
PRELIMINARY ASSESSMENT FORM
FOR SECURITY INCIDENTS OR PERSONAL DATA BREACHES [1]

I. Nature and scope of the incident/ personal data breach

II. Immediate damage or implications of such incident or breach (confidentiality, integrity, availability of personal data)

III. Initial assessment regarding UP's obligation to notify data subjects and the NPC[2] Note that in case of doubt UP must consider whether providing notice to data subjects will enable them to avoid the risk of serious harm[3]

---

[1] This must be accomplished by the head of the incident or breach response team (either UP ITDC Director or head of unit whose data processing system is affected) and transmitted to the UP President and the UP System Data Protection Officer within a reasonable period of time before the 72 hour period counted from notice of the incident or breach to enable UP to make a timely notice to data subjects and the NPC per NPC MC 2016-03. See Secs. 7 and 8 of the Proposed Security Incident and Personal Data Breach Procedures for UP System Offices

[2] UP shall notify the NPC and affected data subjects within seventy two (72) hours from knowledge or reasonable belief that sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and UP or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. 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 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.

[3] Where there is uncertainty as to the need for notification, the concerned office shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, can reduce the risks arising from the personal data breach reasonably believed to have occurred.Such office shall also consider if the personal data reasonably believed to have been compromised involves:**(a)** Information that will likely affect national security, public safety, public order, or public health;**(b)** At least one hundred (100) individuals; **(c)** Information required by applicable laws or rules to be confidential; or**(d)** Personal data of vulnerable groups. 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.

IV . Assessment regarding UP's obligation to notify law enforcement agencies.[4]
V. Recommendation regarding the need for external expertise (including expertise outside of the UP System Administration Offices but which can be obtained from the CUs e.g. faculty or staff who can conduct forensic examinations)

V. What immediate measures have been taken to:
Secure evidence?

Contain the incident or breach?

Restore integrity to the ICT system?

[4] https://www.doj.gov.ph/reporting_cybercrime.html
https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/
https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/