FORM 5
UNIVERSITY OF THE PHILIPPINES
FINAL REPORT OF SECURITY INCIDENT OR PERSONAL DATA BREACH [1]

I. Description of the security incident or personal data breach, its root cause and circumstances regarding its discovery

II. Actions and decisions of the incident response or breach response team[2].

III. Outcomes of the incident/breach management, and difficulties encountered

IV. Compliance with notification requirements and assistance provided to affected data subjects if applicable.

V. Recommendations to address and prevent similar incidents/breaches which may include the revision of this breach response procedure, other policies and procedures, additional stakeholder training, etc.

[1] The UP Data Privacy Manual states:
SECTION 32**.** All actions taken by the University in responding to a security incident or data breach shall be properly documented. All security incidents and personal data breaches shall be documented through written reports (Form 5), including those not covered by the notification requirements. …
All reports shall be submitted to the proper DPO and made available when requested by the NPC:

For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. Any or all reports shall be made available when requested by the NPC: *Provided*, that a summary of all reports shall be submitted to the NPC annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

[2] These must be properly documented through written periodic reports and a final report to be prepared by the head of the security incident or breach response team with the assistance of the data breach response team members. Aside from a narrative report, the measures adopted in order to address the breach need to be documented through, for example, relevant memos, emails, screen shots of actions taken, logs, documents from a relevant third party, sworn statements and the like. Such report and documentation regarding measures done by an office assisting the head of the breach response team must be provided to concerned officers or offices such as the proper Data Protection Officer the UP President and the head of the breach response team for the purpose of enabling UP to comply with the Data Privacy Act and National Privacy Commission issuances.