UNIVERSITY OF THE PHILIPPINES
DILIMAN **QUEZON CITY**
VOIP TRUNKLINE: 981-8500 LOCAL: 2558, 2556
DIRECT LINE: (632) 929-5401, (632) 927-1835
FAX: (632) 928-2863
E-MAIL: chancellor.updiliman@up.edu.ph

OFFICE OF THE CHANCELLOR

11 June 2019

MEMORANDUM NO. MLT-19-149

TO : Deans, Directors, Heads of Units, Faculty, REPS and Staff Information Officers / Data Privacy Compliance Focal Persons

SUBJECT : **UP Diliman Data Privacy Oversight and Review Plan**

To set measures and define roles in the oversight and review of UP Diliman's privacy management program, the attached UP Diliman Data Privacy Oversight and Review Plan is hereby issued.

MICHAEL L. TAN, PhD
Chancellor

University of the Philippines Diliman
Oversight and Review Plan

This document serves as a guide in monitoring, assessing, revising and reporting the effectiveness of the privacy program in UP Diliman.

PART I.
OBJECTIVE AND SCOPE

Objective

The objectives of this document are to:

- Set measures in ensuring that the policies and procedures for data privacy are followed and updated
- Define roles and responsibilities of academic units and administrative offices in the oversight and review of UP Diliman's privacy management program

Scope

This document covers UP Diliman and UP People and all privacy related policies and initiatives promulgated and amended by UP Diliman or any of its units and offices.

Definition of Terms

For the purpose of this document, the following terms are defined, as follows:

1. ***Data Subject*** refers to an individual whose personal information is processed;
2. ***Data Protection Officer or DPO*** refers to a person appointed or designated by UP Diliman to be accountable for ensuring compliance with DPA, its IRR, related issuances of NPC, and other applicable laws and regulations relating to data privacy and security;
3. ***DPA*** refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
4. ***IRR*** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
5. ***NPC*** refers to the National Privacy Commission of the Philippines as created by the Data Privacy Act of 2012;
6. ***Personal Data*** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;

7. ***Privacy Impact Assessment or PIA*** refers to the self-assessment that the NPC Commission mandated for personal information controllers such as UP Diliman. The objected of the PIA is to determine how an organization processes personal information, identify the privacy risks, and manage these risks.
8. ***Privacy Focal Person or PFP*** refers to an academic unit's or administrative office's focal person for data privacy compliance acting as compliance officers for privacy. They are champions of data privacy and agents of pursuing data privacy culture in their unit. A go-to person when it comes to data security and privacy compliance;
9. ***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;
10. ***Staff*** refers to UP Diliman staff, including Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, and retirees as well as UP Diliman Faculty, including visiting faculty;
11. ***UP People*** refers to Staff, researchers, alumni, subcontractors, outsourcees, agents and representatives of UP Diliman;
12. ***Units and Offices*** refers to UP Diliman Academic Units and Administrative Offices.

PART II.
GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPPs)

The Data Protection Officer shall formulate criteria to review the overall privacy program of UP Diliman based on the following GAPPs:

1. **Management**. UP Diliman for its privacy policies and procedures has defined, documents, communicates and assigns accountability.
2. **Notice**. UP Diliman provide privacy notices to UP People which includes the details about the processing of personal information.
3. **Choice and consent**. UP Diliman provides to UP People the rights and responsibilities and obtains Data Subject's consent in processing their personal information.
4. **Processing**. UP Diliman collects and process personal information as compliance to its mandate and legal obligation.
5. **Access**. UP Diliman grants access to Data Subjects to access, review and update their Personal Information.
6. **Disclosure to third parties**. UP Diliman may disclose Personal Information to third party (other than UP People) only for the purpose specified in Contract/Agreement.
7. **Security for privacy**. UP Diliman protects and secure Personal Information against security incident.
8. **Quality**. UP Diliman maintains that the Personal information are accurate, complete and relevant for the purpose of compliance to legal obligation.
9. **Monitoring and enforcement**. UP Diliman monitors the effectiveness of the privacy measures and has procedures in addressing the gaps and concerns.

PART III.
ROLES AND RESPONSIBILITY

Data Protection Officer

The DPO shall actively monitor the following and share the update to UP Diliman's PFP Community:

1. Philippine Laws (e.g. DPA, and its IRR)
2. NPC's Policies and standards
3. UP Diliman's Policies and Standards
4. Academic Unit and Administrative Office's level of privacy compliance
5. Level of Risk in the Processing of Data

The DPO will have the oversight authority as well as review authority on actions and decisions related to the forms, documents and initiatives on data privacy and data protection in UP Diliman, its units and offices and UP People.

Privacy Focal Person

Each Privacy Focal Person has the obligation to update the PIA for all changes in their processing of documents, policies, and data processing systems.

Computer Center

Computer Center will conduct Vulnerability Assessment (with Penetration Testing) for all new and all updated Diliman-wide Data Processing Systems and those of vital offices. The assessment and testing may also be conducted upon request of the units and offices affected by the system and upon the result of the risk assessment made by the DPO.

UP Diliman-Wide Breach Response Team (BRT)

Diliman-wide BRT will make recommendations to DPO based on "Lessons Learned" from security incidents and personal data breaches.

PART IV.
REVIEW SCHEDULE

The Data Protection Officer shall set a specific month for an annual schedule to review the privacy policies and procedures and identify the gaps. These gaps shall be reviewed and be a basis for the update of the document, if necessary.