University of the Philippines Diliman
**Data Protection Team**

upd.edu.ph/privacy

dpo.updiliman@up.edu.ph

(632) 8255-3561

02 January 2020

**MEMORANDUM**

Reference No. EBM 19-03

| | | |
|---|---|---|
| FOR | : | Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons |
| SUBJECT | : | **UP Diliman Data Classification Policy** |

The privacy treatment of documents in UP Diliman should not be arbitrary. To standardize the levels of accessibility and security governing documents and the information they contain, there should be a clear set of parameters on which documents should be restricted and how to implement such restrictions.

In line with the UP Diliman Data Protection Officer's responsibility under Office of the Chancellor Memorandum No. 19-073 to issue data privacy policies, the attached UP Diliman Data Classification Policy is hereby promulgated.

Elson B. Manahan, JD
*Data Protection Officer*

Noted by:

Michael L. Tan, DVM, PhD
*Chancellor*

University of the Philippines Diliman

# DATA CLASSIFICATION POLICY

## I. Scope

This Policy governs all documents and information in UP Diliman whether in physical or electronic format. If needed, a section of a document or file may be given a classification different from the document or file containing it.

## II. Responsibility

Privacy Focal Persons shall be ultimately responsible to ensure that all documents and files in their respective academic units and administrative offices have a classification under this Policy.

## III. Availability

Documents and files, as well as the information contained in them, may either be classified as *restricted* (internal, confidential, or sensitive confidential) or *public*. Examples are:

- Data which are customarily processed by specific UP Diliman units and offices are *restricted* as Internal.
- Personal Information under the Data Privacy Act of 2012 are *restricted* as Confidential.
- Sensitive Personal Information under the Data Privacy Act of 2012 are *restricted* as Sensitive Confidential.
- Citizens' Charters are not restricted and hence are *public*.

## IV. Restricted Data

Access to data in UP Diliman are restricted to varying *classes of users* according to risk level:

A. **Internal** – Data which generally pose a *low risk* to the rights of data subjects and UP Diliman.
B. **Confidential** – Data which generally pose a *medium risk* to the rights of data subjects and UP Diliman.
C. **Sensitive Confidential** – Data which generally pose a *high risk* to the rights of data subjects and UP Diliman.

### IV-A. Internal

Definition: Data which should be internally contained within certain UP Diliman units or offices.

Restriction: May be accessed only by *UP Diliman units or offices* which need such data to perform their roles and responsibilities.

Risk: Low. UP Diliman may incur financial losses, reputational damage, or lose opportunities.

Examples:

- Employee benefits may be accessed by HRDO and Accounting Office but not by unconcerned offices.
- Draft documents not yet cleared for release may not be demanded by other offices.

### IV-B.Confidential

Definition: Information which in may only be disclosed only to a limited number of individuals to protect UP Diliman from legal, regulatory, financial, strategic, operational or reputational risks.

Restriction: May be accessed only by *specific UP Diliman officials, staff or faculty* if the data is necessary to perform an official task.

Risk: Medium. UP Diliman may be incur judicial or administrative liability. Rights of individuals may be violated.

Examples:

- Personal information such as home address, email, and photos.
- Patent application documents.

### IV-C. Sensitive Confidential

Definition: Information that may likely cause serious harm to UP Diliman or individuals if not strictly protected.

Restriction: May be accessed on a need-to-know basis only by *the minimum number of UP Diliman officials, staff or faculty* whose knowledge of the information is highly necessary to address a need.

Examples:

- Sensitive personal information such as age, political affiliation, health, education, and government-issued I.D. numbers.
- Privileged information such as those in sexual harassment cases disclosed to officials, adjudicators, lawyers and doctors.

## V. Public Data

Public data should be freely accessible to parties internal and external to UP Diliman. Except for reasonable procedural requirements, there should be no restrictions to access public data.

In requests invoking the freedom of information, the procedure in the UP Diliman Freedom of Information Manual should be followed.

## VI. Security Measures

Whether restricted data or public data, appropriate physical, organizational and technical security measures in the UP Diliman Privacy Manual and other relevant rules should be complied with.