University of the Philippines Diliman
Data Protection Office

upd.edu.ph/privacy
dpo.updiliman@up.edu.ph
(632) 8255-3561

22 July 2020

MEMORANDUM

UPD DPO Memorandum No. EBM 20-**14**

FOR : Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons

SUBJECT : **UP Diliman Data Governance Policy**

The University of the Philippines Diliman recognizes the need to uphold the quality and integrity of personal information, including sensitive personal information and privileged information that it processes in the fulfillment of its mandate and legal obligations as an educational institution and government instrumentality.

In order to achieve this, there is a need to establish an accountability framework to ensure that proper measures are observed in the handling and usage of data. In line with this, the attached Data Governance Policy is hereby adopted.

Digitally signed by
84ea024e-fb7a-4132-a4e6-2609948aaa75
Reason: PNPKI digital signature legally recognized by R.A.8792

Elson Manahan
Data Protection Officer

University of the Philippines Diliman
DATA GOVERNANCE POLICY

I. Preliminary Provisions

Section 1. *Objectives* – This Data Governance Policy (*Policy*) aims to:

a. Define the roles and responsibilities for different data usage and establish clear framework of accountability;

b. Develop best practices for effective data management and protection;

c. Protect the University of the Philippines Diliman's (*University*) data against internal and external threats (e.g., breach of privacy and confidentiality);

d. Ensure that data used by the University in its decision making, reporting, and planning, are complete, accurate, and unaltered;

e. Ensure the University's compliance with applicable laws, regulations, and standards and mitigate compliance risks; and

f. Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, reporting, managing and storing of data

Section 2. *Scope* – This policy applies to all personal data, including sensitive personal information and privileged information, that are processed, used, or handled by the concerned UP People.

This Policy is in line with the UP Diliman Data Classification Policy,[1] Records Management Policy,[2] and UP Diliman Privacy Manual.[3]

Section 3. *Definition of Terms* – For the purpose of this Policy, the following terms are defined as follows:

a. ***Access*** – refers to the finding, retrieval, or use of data;

b. ***Confidential data*** – refers to information that may be disclosed only to a limited number of UP Diliman Staff for the performance of their official tasks;[4]

c. ***Document Administrator*** – refers to the person in-charge in a unit or office that has the authority to generate, release, keep or revise a document.

d. ***Document User*** – refers to the director, officer, employee, or requesting party that accesses or utilizes a document;

---

[1] UP Diliman Data Protection Office Memorandum No. EBM 19-03, 02 January 2020; UP Diliman Data Protection Office Memorandum No. EBM 20-06, 11 May 2020
[2] UP Diliman Data Protection Office Memorandum No. EBM 20-07, 26 May 2020
[3] UP Diliman Data Protection Office Memorandum No. EBM 19-02, 11 November 2019
[4] *See* Data Protection Team Memorandum Reference No. EBM 19-03 dated 2 January 2020

e. ***Documents*** – refers to forms, templates, records, lists, tables, reports, issuances, invoices, receipts, or other documents that contain personal information of data subjects, whether in printed or electronic format;

f. ***Personal Data*** – refers to personal information as defined in Republic Act No. 10173 or the Data Privacy Act of 2012;

g. ***Privacy Focal Person*** – refers to an academic unit or administrative office's point person for data compliance;

h. ***Private Information*** – refers to personal and confidential data;[5]

i. ***Units and Offices*** – refer to University of the Philippines Diliman academic units and administrative offices;

j. ***UP People*** – refers to students, parents, guardians, faculty, visiting faculty, staff, Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, retirees, applicant students, applicant faculty, applicant staff, researchers, research subjects, patients, clients, customers, alumni, donors, donees, contract counterparties, partners, subcontractors, outsourcees, licensors, licensees and other persons with a juridical link with UP Diliman

II. Data Governance: Inventory and Classification

Section 4. ***Inventory*** – The conduct of a data inventory is the preliminary step in ensuring the protection and integrity of personal data. Before data can be classified and be given the appropriate security measures, each unit and office must first identify all the documents that it administers.

Section 5. ***Classification*** – After a determination of the documents it administers, units are to classify them in accordance with the UP Diliman Data Classification Policy.[6]

Under the UP Diliman Data Classification Policy, documents in the University are classified in terms of availability:

a. *Public* – Documents that are deemed freely accessible to parties that are both internal and external to the University, subject to reasonable procedural requirements (e.g., Information requests under the Freedom of Information)

   This also includes non-sensitive matters such as but not limited to open data, publicly available information including informational websites, terminology systems, standards, practitioner registries, classified and treated as such under "Tier 1" of the Department of Information and Communications Technology Department Circular No. 2017-002, Prescribing the Philippine Government's Cloud First Policy.[7]

b. *Restricted* – Documents that are deemed to be accessible only to a limited group or number of individuals.

[5] Office of the Chancellor Memorandum Reference No. MLT 18-135, dated 23 May 2018
[6] *See* Note 1
[7] DICT Department Circular No. 2012-02, as amended by Department Circular No. 2020-010 also prescribes a classification for data owned or processed by the Government

Restricted Data can further be classified into the following categories, according to their corresponding risk levels:

i. *Internal data* – refers to data which generally pose a *low risk* to the rights of data subjects and the University.

   It should be internally contained within the University's colleges and offices and may be accessed only by such offices and colleges which need such data to perform their roles and responsibilities.

ii. *Confidential data* – refers to data which generally pose a *medium risk* to the rights of data subjects and the University.

   The University may incur judicial or administrative liability and rights of individuals may be violated. As such, it may be disclosed only to a limited number of individuals to protect the University from legal, regulatory, financial, strategic, operational or reputational risks, and may be accessed only by *specific directors, deans, officers, or employees* if the data is necessary to perform an official task.

   Internal and Confidential Data likewise includes restricted matters, such as but not limited to students' data, email, and CRM systems. Examples include financial records and medical records such as personally identifiable education records, personally identifiable financial information (PIFI), protected health information. These are classified accordingly as "Tier 2" under the aforementioned DICT Circular.[8]

iii. *Sensitive Confidential data* – refers to data which generally pose a *high risk* to the rights of data subjects and the University and may likely cause serious harm to the students, faculty or individuals if not strictly protected.

   It may be accessed only on a need-to-know basis only by *the minimum number University directors, deans, officers, or employees* whose knowledge of the information is highly necessary to address an operational need.

   These likewise include political documents dealing with matters of international negotiations, technical matters of military value, major governmental projects such as proposals to adjust the nation's economy (before official publication) internal audit data, trade secrets, technical data supporting technology transfer agreements. These are classified accordingly as "Tier 3" under the aforementioned DICT Circular.[9]

For reference, below are the different classifications of data under the UP Diliman Data Classification Policy, *vis-à-vis* its equivalent classifications under the DICT Cloud First Policy.

[8] Ibid
[9] Ibid

UP Diliman Data Classification Policy Categories	DICT Cloud First Policy Categories
Public	Tier 1
Restricted – Internal	Tier 2
Restricted – Confidential	
Restricted – Sensitive Confidential	Tier 3

It must be stressed the providing the proper classification for data allows the unit or office to determine the appropriate security measures to protect it from privacy risks or threats, while ensuring its accessibility and availability to authorized parties.

III. Data Governance: Responsibilities of Document Administrators and Users

Section 6. ***Privacy and Confidentiality*** – All directors, officers, employees, agents, sub-contractors, partners, and counterparties are responsible to uphold the privacy and confidentiality of all documents and information under this Policy.

Section 7. ***Document Classification*** – Heads of departments, units, or offices, together with their respective Privacy Focal Persons (PFPs) shall ensure that all the documents and files administered by their department, office, or unit are classified in accordance with this Policy and the UP Diliman Data Classification Policy.

Section 8. ***Compliance with Policies*** – All UP People are responsible in ensuring the privacy and confidentiality of the documents and information that they use and process. Furthermore, they are to ensure that the privacy and security measures prescribed by the UP Diliman Information Security Policy[10], UP Diliman Data Privacy Manual, and other pertinent issuances.

Section 9. ***Communications*** – All UP People are responsible in ensuring the privacy and confidentiality of all messages and communications, in whatever format, that is received or transmitted through their respective units and offices. Observance of the UP Diliman Message and Communication Policy[11] is strictly enjoined.

Thus, private information contained in messages or correspondences, whether in sealed envelopes or otherwise, are deemed as strictly confidential and intended to for the addressee(s) only. Therefore, all UP People are to refrain from opening and/or reading messages, communications, or correspondences, in whatever format, that are intended for others.

Section 10. ***Document Administration*** – The unit or office Document Administrator has responsibility to enforce the application of this Policy to a specific document. This responsibility rests in the unit or office's respective deans or directors.

Section 11. ***Document Use*** – All document users are responsible for ensuring the privacy, confidentiality, and integrity of the documents that they use.

[10] UP Diliman Memorandum No. EBM 20-09, 09 June 2020

[11] Office of the Chancellor Memorandum No. MLT 18-135, 23 May 2018

Section 12. *Document Access* – Unit and office heads, together with their PFPs, are responsible in determining the authorized persons that are to be granted access to documents, through the creation of access restrictions or guidelines.

In prescribing the levels of accessibility of documents, reference to the UP Diliman Data Classification Policy is strongly advised.

Section 13. *Document Storage* – In line with the provisions of the UP Diliman Records Management Policy,[12] all units and offices are expected to provide a proper storage device and/or location for their documents.

In addition, these storage devices or spaces must be secured in such a way that its contents cannot be accessed by unauthorized persons. Provided, however, that the availability of the same to authorized persons will not be hampered.

Section 14. *Document Disposal and Destruction* – Every unit or office must be guided by the general principle that data should be retained only for as long as it is necessary for the legitimate purpose for which the data were collected.[13]

Thus, as long as there remains to be a legitimate purpose for retaining the collected data, then the retention of the same is allowed. Each unit or office is expected to implement the appropriate security measures in record retention.

In line with the UP Diliman Records Management Policy, documents are to be appraised to determine its value for future use, for whatever purpose, and the period the said value will remain.

In disposing of documents, including excessive copies thereof, the following requisites must be complied with:

a. The documents must be destroyed in such a way that the data therein cannot be reconstituted (e.g., shredding, burning, pulping);
b. There is no law or regulation requiring the continued use or retention of the document;
c. UP Diliman has no foreseeable indispensable need for the document; and
d. No data subject rights shall be violated.

Section 15. *Document Retention* – Reference to the following issuances are highly encouraged in determining the periods for the processing, which includes the retention and disposal, of personal data:

1. The Data Privacy Act of 2012, its Implementing Rules and Regulation, and relevant issuances of the National Privacy Commission;
2. The National Archives of the Philippines Act of 2007, its Implementing Rules, and relevant issuances of the National Archives of the Philippines;
3. Policies, guidelines, and rules of the UP System and UP Diliman;
4. Research guidelines and Ethical Codes of Conduct adopted by the University of the Philippines Diliman; and
5. Executive Order No. 2, series of 2016 on Freedom of Information and subsequent related executive orders and laws.

[12] UP Diliman Data Protection Office Memorandum No. EBM 20-07, 26 May 2020
[13] Sec. 11 (e), Chapter III, R.A. No. 10173

In the absence of applicable rules on retention, personal data shall be retained and disposed by units and offices in accordance with the practices of government agencies with analogous functions.

Section 16. ***Back-up and Protection*** – In order to ensure the availability and protection of documents, document users and administrators are highly encouraged to refer to the Back-up Policy provided in the UP Diliman Information Security Policy.[14]

Section 17. ***Security Incident and Personal Data Breaches*** – In line with the UP Diliman Data Privacy Security Incident Management Policy,[15] Breach Response Teams in the Constituent University-Level (Diliman-Level Breach Response Team) and Unit or Office-level (Unit-Level Breach response Teams) are to be constituted.

These teams are responsible for assessing and evaluating security incidents, including personal data breaches, involving the documents within their jurisdiction. They are also responsible for restoring integrity to the information contained therein, mitigating and remedying the resulting damages, and complying with reportorial requirements.

IV. Policy Review and Support

Section 18. ***Policy Review*** – This Policy will be reviewed and updated annually from the approval date, or as may be necessary. As such, any employee, officer, director or dean who wish to make any comments about the Policy may forward their suggestions to the UPD Data Protection Office for discussion and possible modification of this Policy.

Section 19. ***Support*** – Any employee, officer, director or dean requiring assistance in the construction, implementation, and over-all interpretation and application of this Policy may seek the assistance of their respective Privacy Focal Persons. Should further assistance be needed, the concerned party should contact the UPD Data Protection Officer for clarification

[14] *See* Note 10.

[15] Office of the Chancellor Administrative Order No. MLT 19-072, 25 March 2019