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*** 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 admi

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.

   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

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 theAll UP Peoplo9