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-**13**

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

SUBJECT : **UP Diliman Organizational and Physical Security Policy**

Organizations tend to invest in I.T. infrastructures to secure their data. However, studies reveal that majority of security incidents and data breaches are due to human error. To minimize vulnerabilities in the relational structure and manual processing of personal data, the attached UP Organizational and Physical Security Policy is hereby promulgated.

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

ORGANIZATIONAL AND PHYSICAL SECURITY POLICY

The University of Philippines Diliman recognizes that the proper management, including the safekeeping, and use of information is a vital factor to the University's operations to fulfill its mandate.

To achieve this, herein Organizational and Physical Security Policy is hereby adopted.

I. Preliminary Provisions

Section 1. *Objective* – This Policy shall serve as a guide on what is incumbent upon the UP People to undertake in order to ensure the availability, integrity, and confidentiality of information, including personal data, as well as to secure the same from natural and man-made dangers, and unauthorized processing.

Section 2. *Scope* – This Policy applies to all concerned UP People involved in the creation, management, and use of data, stored in UP Diliman's data processing systems, in their dealings with the University.

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. ***Computing Assets*** – refers to the personal computers, workstations, laptops, netbooks, storage devices, tablets, servers, and smart phones;

c. ***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;[1]

d. ***Documents*** – refers to forms, templates, records, lists, tables, reports, issuances, invoices, receipts, or other documents that contain personal information of data subjects;

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

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

g. ***Private Information*** – refers to personal and confidential data;[2]

h. ***Processing of data*** – refers to any operation or any sets of operations performed upon data, such as, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, and erasure or destruction;

---

[1] *See* Data Protection Team Memorandum Reference No. EBM 19-03 dated 2 January 2020

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

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

j. ***UP Diliman*** – refers to the University of the Philippines Diliman;

k. ***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. Organizational Security Measures

Section 4. ***Data Access*** – Access to a particular type of data shall be determined based on its classification under the UP Diliman Data Classification Policy.[3]

Access to any data owned by UP Diliman shall only be granted to authorized UP People with a legitimate purpose for the same. Furthermore, they must refrain from gaining unauthorized access or exceeding the authorized access to the data granted to them.

In accessing the data, the concerned UP People must maintain the quality and integrity of the same.

Units and offices providing access to the data in their custody must ensure that proper access controls, such as access logs, are maintained to document the movement of the data.

Section 5. ***Data Collection*** – The data collected by UP People must not be excessive for the legitimate purpose for which it was intended.

Thus, prior to providing any requested data, it is incumbent upon the concerned UP People to determine if the request is for a legitimate purpose and not contrary to any rules and regulations promulgated by UP Diliman.

Section 6. ***Data Usage and UP Diliman's Usage Policy*** – The use of data shall only be granted to authorized UP People with a legitimate purpose for the same. Consequently, any disclosure or transfer of data must be only in the pursuance of their official functions.

All UP People using the data must use the same strictly for its intended purpose only. Furthermore, they must refrain from performing any act that would amount to the unauthorized use of the data or exceeding the authorized use of the same. In using the data, the concerned UP People must likewise ensure that the quality and integrity of the same is preserved.

Furthermore, copyright, licenses, and intellectual property rights must be observed and respected in the course of the use of the data. Thus, users are strictly enjoined to not infringe on the copyright and other property rights covering the data that is the subject of their use.

In addition thereto, all UP People accessing and/or using data within the premises of UP Diliman through its computing facilities, networks and other information technology

[3] *See* Note 1

resources are enjoined to abide by the Acceptable Use Policy for Information Technology Resources of the UP System.[4]

Units and offices providing access to the data in their custody must ensure that proper usage controls, such as logs, are maintained to document the movement of the data.

Section 7. ***Privacy*** – All UP People accessing and processing data must do so under strict confidentiality, in order to ensure that any internal, confidential, or sensitive confidential information will not be disclosed to unauthorized persons.

Section 8. ***Privacy Focal Persons*** – Privacy Focal Persons are designated by the Office of the Chancellor to coordinate and assist the UP Diliman Data Protection Team in its endeavors; implement privacy policies and initiatives; monitor, mitigate, and manage foreseeable security incidents and personal data breaches in their respective units and offices; and investigate, address, and resolve privacy gaps in their respective units and offices.[5]

Section 9. ***Messages and Communications*** – UP People creating, sending, transmitting, receiving, accessing, using, processing, and storing messages and communications, whether in print or electronic format, must ensure that the private information therein is maintained and kept confidential. Furthermore, they must ensure that the same will be for the intendent parties therein only.

Section 10. ***Consent to the Processing of Personal and Private Information*** – The processing of any personal or private information shall require the consent of the data subject.

In crafting consent notices or forms, the right of the data subject to be informed and create an intelligible decision must be of paramount importance.

Section 11. ***Responsibility of UP People*** – Acts and decisions of UP People with respect to any information that they process in relation to their dealings with UP Diliman must be in line with the UP Diliman Privacy Manual.[6]

Moreover, in the conduct of their affairs, UP People are to abide by the three cardinal principles of privacy to ensure that data is at all times protected:

a. ***Transparency*** – Data subjects to be informed of the nature, purpose, and extent of the processing of their personal data;
b. ***Legitimate Purpose*** – The data must be processed only for the purpose for which it was intended, provided that the same is not contrary to laws, morals, and public policy. Moreover, the consent for the processing must be freely given by the data subject;
c. ***Proportionality*** – The data processed must not be excessive in relation to the declared purpose. Thus, only the pertinent data should be processed.

Furthermore, UP People are strictly enjoined to refer and abide by the UP Diliman Privacy Policy and UP Diliman Data Subject Rights and Responsibilities.

[4] https://upd.edu.ph/wp-content/uploads/2019/03/AUP.pdf
[5] *See* Office of the Chancellor Memorandum Reference No. MLT 18-022 dated 15 January 2018
[6] Data Protection Team Memorandum Reference No. EBM 19-02

Section 12. *Security Incidents* – In the event of a security incident or data breach, units and offices must abide by the guidelines provided in the UP Diliman Security Incident Management Policy.[7]

III. Physical Security Measures

Section 13. *Data Format* – Data accessed, collected, and processed, whether in print or electronic format, must be kept secure by all UP People concerned.

Section 14. *Storage* – Data storage devices such as, but not limited to, folders, envelopes, drawers, filing cabinets, vaults, rooms are kept within the premises of UP Diliman and/or storage facilities contracted by UP Diliman.

Section 15. *Storage Access* – Access to the data storage facilities shall be subject to the following restrictions:

a. Only authorized UP People are allowed to enter the premises where data is kept. The unit, office, or facility where the data is stored is tasked to maintain an access log wherein the entry and exit, and purpose of access to the storage facility will be recorded;
b. The building and the surrounding premises where the storage devices are kept shall be monitored by a closed circuit television (TV) that will capture and record the identity and actions of the persons that will access the said storage devices; and
c. UP People accessing, using, or processing data are responsible to keep the same secured from any form of unauthorized use and access. Thus, they must ensure that the storage devices such as cabinets and drawers are kept locked; and folders and envelopes are sealed.

Section 16. *Security of Computing Assets and storage devices* – Owners and authorized holders and users of computing assets are responsible for the safety of the same. Everyone is expected to practice due diligence in keeping the said assets safe from unauthorized access, use, theft, loss, or destruction due to various causes.

a. *Fire and power* – Owners, users, and holders must be mindful of the places where they will place their computing assets. They must ensure that the area is secured and not a fire hazard.

   Smoke detectors and fire extinguishers and sprinkler systems, when applicable, must be provided in every unit and office.

   If necessary and practicable, the use of an uninterrupted power supply (UPS) is highly encouraged to ensure that the computing assets will continue to function in the event of a power outage. Backup generators are also highly advised to be used by units and offices in order for the same to continue with their operations should electricity be lost. Voltage regulators, when applicable, must also be used to ensure that the computing assets are kept safe from voltage surges.

b. *Temperature and humidity* – Units and offices must ensure that the temperature and humidity are within the proper range to ensure that the assets and devices will not overheat or be subject to corrosion.

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

c. *Water* – Computing assets and storage devices must be placed in a location safe from water damage. If the unit or office is situated in an area prone to flood, it is advisable that the assets or devices be stored in a remote site instead.

   Units and offices must ensure that their premises is not susceptible to leakage which may not only cause damage to the assets and devices but may also endanger the people should electrocution occur.

Section 17. *Workspaces*– Heads of units and offices must ensure that their staff's workspaces in such a manner that the privacy of the data that they process is maintained. Documents, files, and monitors must also be arranged in a way that it cannot be viewed by unauthorized persons.

Documents containing confidential or sensitive confidential data must not be left exposed on one's workstation. Moreover, UP People are mandated to keep away the said documents from visitors to avoid any unauthorized access, use, or copying of confidential or sensitive confidential data.

Section 18. *Documents Disposal* – Units and offices must refer to the UP Diliman Records Management Policy and the pertinent issuances of the National Archives of the Philippines in disposing their documents.

It is incumbent upon UP People to exercise due diligence in the disposal of their documents. When possible, the documents must be shredded or destroyed, in order to ensure that any information contained therein can no longer be reconstituted.