UP DILIMAN DATA PROTECTION OFFICE

ORGANIZATIONAL SECURITY MEASURES

Source: UPD DPO MEMORANDUM No. EBM 20-13

SEC. 4 DATA ACCESS

Access to a particular type of data shall be determined based on its classification under the UP Diliman Data Classification Policy.

SEC. 5 DATA COLLECTION

Determine if the request is for a legitimate purpose and not contrary to any rules and regulations.

SEC. 6 DATA USAGE AND UP DILIMAN'S USAGE POLICY

All UP People using the data must use the same strictly for its intended purpose only.

SEC. 7 PRIVACY

All UP People accessing and processing data must do so under strict confidentiality.

SEC. 8 PRIVACY FOCAL PERSONS

Privacy Focal Persons or PFPs are designated by the Office of the Chancellor to coordinate and assist the UP Diliman Data Protection Team in its endeavors.

SEC. 9 MESSAGES AND COMMUNICATIONS

UP People must ensure that the private information in messages and communications is maintained and kept confidential.

SEC. 10 CONSENT TO THE PROCESSING OF PERSONAL AND PRIVATE INFORMATION

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.

SEC. 11 RESPONSIBILITY OF UP PEOPLE

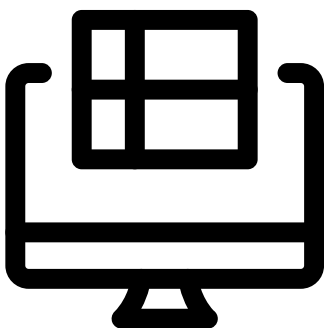
UP People are to abide by the three cardinal principles of privacy to ensure that data is at all times protected: ***Transparency, Legitimate Purpose, and Proportionality.***

SEC. 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.

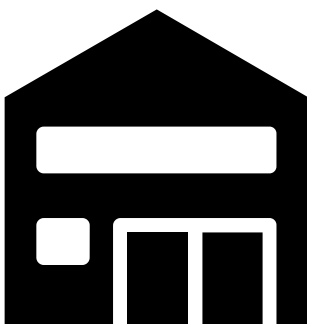
UP Diliman Data Protection Office

PHYSICAL SECURITY MEASURES



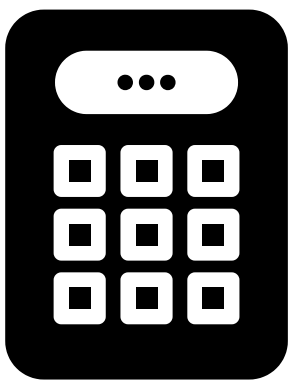
1 DATA FORMAT

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



2 STORAGE

Data storage devices are kept within the premises of UP Diliman and/or storage facilities contracted by UP Diliman.



3 STORAGE ACCESS

- Only authorized UP People are allowed to enter the premises where data is kept
- The building and the surrounding premises where the storage devices are kept shall be monitored by CCTV.
- UP People must ensure that the storage devices such as cabinets and drawers are kept locked; and folders and envelopes are sealed.

4 SECURITY OF COMPUTING ASSETS AND STORAGE DEVICES

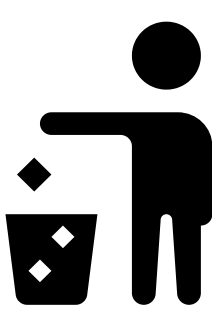
- Ensure that the area is secured and not a fire hazard.
- Smoke detectors and fire extinguishers and sprinkler systems must be provided.
- UPS is highly encouraged.

- Ensure that the assets and devices will not overheat or be subject to corrosion

- Computing assets and storage devices must be placed in a location safe from water damage.

5 WORKSPACES

Documents, files, and monitors must be arranged in a way that it cannot be viewed by unauthorized persons.



6 DOCUMENTS DISPOSAL

Refer to UP Dilian Records Management Policy and exercise due diligence in the disposal of the documents.

Source: UPD DPO MEMORANDUM No. EBM 20-13