UP DILIMAN DATA PROTECTION OFFICE

INFORMATION SECURITY POLICY

CHAPTER IX
PERSONAL DATA BREACH MANAGEMENT

RISK

a potential cause of an unwanted incident which may result in harm to a data subject, system, or organization

THREAT

a potential cause of an unwanted incident which may result in harm to a data subject, system, or organization

VULNERABILITY

weakness of a data processing system that makes it susceptible to threats

The performance of a series of risk assessment activities will allow units and offices to determine the likelihood of a threat exploiting a vulnerability of a process and its possibility of resulting to a risk. This series of activities include:

1. IDENTIFY OR ASSESS THE DATA PROCESSING ACTIVITIES AND SYSTEMS OF A UNIT
2. IDENTIFY THE POSSIBLE THREATS THAT MAY TRIGGER OR EXPLOIT THE WEAKNESSES OF THE DATA PROCESSING ACTIVITIES AND SYSTEMS OF A UNIT
3. IDENTIFY THE POSSIBLE VULNERABILITIES OR WEAKNESSES IN THE DATA PROCESSING ACTIVITIES OR SYSTEMS OF THE UNIT

Source: Memorandum Reference No. EBM 20-09 UP Diliman Information Security Policy

upd.edu.ph/privacy

UP DILIMAN
DATA PROTECTION OFFICE

INFORMATION SECURITY POLICY

CHAPTER XII

STORAGE DEVICE POLICY, MOBILE DEVICE POLICY, BRING YOUR OWN DEVICE (BYOD) POLICY, CLOUD POLICY

Generally, UP Staff and Faculty may not save work-related files to their personal devices. However, a file may be locally saved to a personal device for only as long as it is necessary to edit the file. Once the edited file has been sent via email or uploaded to a repository, it must immediately be deleted permanently from the personal device.

Only official UP cloud storages may be used for private or confidential information. Cloud users should undertake the appropriate security measures to protect their accounts. They are highly encouraged to create strong passwords and employ, if applicable, a multi-factor authentication system.

CHAPTER XIII

FIREWALLS, ANTIVIRUS SOFTWARES, INTRUSION DETECTION SYSTEMS, OS PATCHES, AND PENETRATION TESTING

Units and offices are strictly prohibited from using pirated software on their official devices such as laptops, workstations, and servers.

The UP Diliman Computer Center, in coordination with the respective units and offices, must ensure that secure and standard configurations are employed for the hardware of the latter's official devices.

Source: Memorandum Reference No. EBM 20-09 UP Diliman Information Security Policy