University of the Philippines Diliman
Data Protection Office

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

09 June 2020

MEMORANDUM

Reference No. EBM 20-09

FOR	:	Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons
SUBJECT	:	**UP Diliman Information Security Policy**

In today's information age, UP Diliman has vast and deep seas of data that demand protection. It is imperative to secure the confidentiality, integrity, and availability of the information created, altered, stored, transmitted, and destroyed by UP Diliman's information systems.

In line with the UP Diliman Data Protection Officer's responsibility to issue privacy policies under Office of the Chancellor Memorandum No. MLT 19-073, the attached Information Security Policy is hereby promulgated.

(Sgd.) Elson Manahan, JD
Data Protection Officer

(Sgd.) Michael Laxina, CPA
Data Privacy Auditor

University of the Philippines Diliman
Information Security Policy

Table of Contents

Objective 5
Scope 5
Definition of Terms 5
Chapter I – Data Governance, Management and Retention Policy 6
Section 1: Data Inventory 6
Section 2: Data Stewardship 7
Section 3: Data Classification 7
Section 4: Retention and Disposal Policy 8
Chapter II – System and Data Access and Control Policy 9
Section 1: Access 9
Section 2: Online Access to Personal Data 10
Section 3: Remote Access 11
Section 4: Remote Disconnection and Wiping 11
Section 5: Guest Access, Separate Guest Network, Third-Party Connection 12
Section 6: Virtual Private Network (VPN) 12
Chapter III – Communications and Email Policy 12
Section 1: Messages and Communications 12
Section 2: Transfer of Personal Data 13
Emails 13
Personal Productivity Software 15
Portable Media 15
Fax Machines 16
Section 3: Email Management – Archiving and Deletion 16
Chapter IV – Website and Cookie Policy 17
Chapter V – Acceptable Use Policy 17
Chapter VI – Password/Passphrase Policy 18
Chapter VII – Backup Policy 19
Section 1: What to back up 19
Section 2: How to back up 19
Section 3: Data Recovery Capability 19
Chapter VIII – Technical Incident Response and Reporting Policy 20
Chapter IX – Personal Data Breach Management 20
Section 1: Security Incident Management Policy 20
Section 2: Threats, Risks, and Vulnerabilities 20
Section 3: Data Breach Response Team 22
Chapter X – Wireless Policy and Network Security Policy 23
Section 1: Network Security Policy 23
Section 2: Wireless Policy 24
Chapter XI – Encryption Policy 24
Section 1: Encryption Standard 25
Section 2: Encryption of Computing Assets 25
Section 3: Encryption of Personal Information 26
Chapter XII – Storage Device Policy, Mobile Device Policy, Bring Your Own Device (BYOD) Policy, Cloud Policy 27
Section 1: Storage Device Policy 27
Section 2: Mobile Device Policy 27

Section 3: Cloud Policy....28
Chapter XIII – Firewalls, Antivirus, Intrusion Detection System, OS Patches, Penetration Testing 28
Section 1: Inventory of Authorized and Unauthorized Devices....28
Section 2: Standard Configurations for Hardware and Software on Laptops, Workstations and Servers....29
Chapter XIV – Recognition of Electronic Documents and Electronic Signatures; Handling of Electronic Evidence 29
Section 1: Recognition of Electronic Documents 29
Section 2: Recognition of Electronic Signatures 30
Section 3: Handling of Electronic Evidence 30

OBJECTIVE AND SCOPE

Objective

The objectives of this document are to:

- Establish measures to protect information and information systems in UP Diliman.
- Ensure confidentiality and integrity while keeping the availability of UP Diliman's information and data.

Scope

The policy governs processing of all data and information flowing to, within and out of UP Diliman as well as all information and computer systems accessed, used or owned by UP Diliman, including hardware, software and their connectivity.

Definition of Terms

For the purpose of this document, the following terms are defined, as follows:

1. ***Computing Asset*** refers to hardware or software used in information processing including operating systems, cloud storage, phones, personal computers, servers, storage devices, etc.;
2. ***Documents*** refer to forms, templates, records, lists, tables, reports, issuances, invoices, receipts, or other documents that contain personal information of individual;
3. ***Electronic document*** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored processed, retrieved or produced electronically;[1]
4. ***Electronic evidence*** refers to an electronic document or electronic data message that is offered or used in evidence;[2]
5. ***Electronic signature*** refers to any distinctive mark, characteristics and/or sound in electronic form. Representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedure employed or adopted by a person and executed or adopted by such person with the intention of authenticating, signing or approving an electronic data message or electronic document;[3]
6. ***Personal Data*** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;

[1] Section 1 (h), Rule II, Rules on Electronic Evidence, A.M. No. 01-7-01-SC
[2] Sec. 1, Rule I, Rules on Electronic Evidence, A.M. No. 01-7-01-SC
[3] Sec. 1 (j) Rule II, Rules on Electronic Evidence, A.M. No. 01-7-01-SC

7. ***Privacy Focal Person (PFP)*** refers to the individual designated by a UP Diliman unit or office to implement data protection and information security measures. They are champions of privacy and agents in cultivating a culture of respect for privacy;[4]
8. ***Processing*** refers to any operation or sets of operations performed upon personal data, including but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data;[5]
9. ***Units and Offices*** refer to UP Diliman Academic Units and Administrative Offices;
10. ***Security Clearance*** is an authority issued by the Office of the Chancellor granting a ss access to sensitive personal information under its control or custody. A security clearance shall only be issued when the performance of the staff's official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the said type of data is allowed.
11. ***Staff and Faculty*** refers to UP Diliman staff, regardless of rank or employment status, including Research, Extension and Professional Staff and Faculty (REPS), UP contractual personnel, Non-UP contractual personnel, and retirees, as well as UP Diliman Faculty, regardless of rank or employment status, including visiting faculty;
12. ***UP People*** refers to Staff and Faculty, faculty, researchers, alumni, subcontractors, students, outsourcees, agents and representatives of UP Diliman.

Chapter I – Data Governance, Management and Retention Policy

Section 1: Data Inventory

The first step in protecting personal data as well as the systems that process them is knowing what data one's office or unit processes. Its identification allows the office or unit it to better ascertain the risks that may be encountered, and thereafter, mitigate if not avoid the same.

Data Inventory is a preliminary step in conducting a Privacy Impact Assessment. In this process, the unit or office identifies the different personal data it collects, its source, and the persons responsible and accountable for the information.

The following questions may serve as a guide when conducting a Data Inventory of personal information:

- Does this material contain personal information?
- How does the unit or process this personal data?
- Where did this data come from?
- How was this obtained by our unit or office?
- Where is this data stored?
- How is this data stored?

[4] 15 January 2018 Office of the Chancellor Memorandum No. MLT 18-022, See UP Diliman Data Privacy Frequently Asked Questions (https://upd.edu.ph/wp-content/uploads/2019/05/Data-Privacy-FAQs-2.pdf)
[5] Sec. 3 (j), Republic Act No. 10173, or the Data Privacy Act of 2012

- Who is in charge with this particular data?

Section 2: Data Stewardship

The protection of data processed by UP Diliman does rest solely in the hands of the Data Protection Team. UP Diliman, as personal information controller (PIC), has designated a Data Protection Officer (DPO) to ensure this institutions compliance with the Data Privacy Act of 2012 (DPA of 2012).[6]

UP Diliman is comprised of various academic units and administrative offices, Privacy Focal Persons (PFPs) were also designated to assist the DPO and the Data Protection Team to, among others, coordinate and assist the latter with complying with the rules and regulations pertaining to the Data Privacy Act.[7]

The designation of the aforementioned personnel is part of data stewardship, a practice where individuals are identified and held accountable for ensuring that units and offices in UP Diliman comply with the DPA of 2012 as well as all other pertinent laws and issuances, and ensure that the personal data that they hold remain protected.

Section 3: Data Classification

After knowing the various personal data a unit or office holds, the next step towards ensuring that these data are protected is to classify them.

The Revised UP Diliman Data Classification Policy (DPO Memorandum No. EBM 20-06) governs the classification levels of documents, files, as well as the information stored therein, whether in physical or electronic format.

In this policy, documents in UP Diliman are classified in terms of their availability: Public and Restricted.

Public data is made freely accessible to parties both internal and external to UP Diliman. Except for reasonable procedural requirements, there should be no restrictions to access public data.[8]

Restricted data, on the other hand, is further classified into three categories:

> First, Internal data should be internally contained within UP Diliman units or offices. it may be accessed only by UP Diliman units or offices which need such data to perform their roles and responsibilities.
>
> Second, Confidential data is information which may be disclosed only to a limited number of individuals to protect UP Diliman from legal, regulatory, financial, strategic, operational

[6] 25 March 2019 Office of the Chancellor Administrative Order No. MLT-19-073
[7] *Supra* Note 4.
[8] Part V. Public Data, Revised Data Classification Policy, Memorandum Reference No. EBM 20-06 dated 11 May 2020.

or reputational risks. It may be accessed by specific UP Diliman Officials, staff, or faculty, provided that the data is necessary for them to perform their official tasks.

Third, Sensitive Confidential Information is data that may likely cause serious harm to UP Diliman or individuals if not strictly protected. It may be accessed only by a minimum number of UP Diliman officials, faculty, staff on a need-to-know basis and their knowledge thereof is highly necessary to address a particular need.

The responsibilities in classifying documents and processing data in accordance with their document classification are as follows:[9]

a. Privacy and Confidentiality – All UP People who are processing Documents are responsible to uphold the privacy and confidentiality of data under this Policy.
b. Document Classification – Privacy Focal Persons shall be ultimately responsible to ensure that all Documents and files *administered* by their unit or office have a classification under this Policy.
c. Compliance with Policies – All UP People shall be responsible to ensure all Documents used by them are kept private and confidential under all privacy policies of UP Diliman.
d. Document Administration – UP Diliman academic unit or administrative office that has authority to generate or revise a Document is considered to be the Document Administrator of such Document. The Document Administrator has responsibility to enforce the application of this Policy to a specific Document.
e. Document Use – UP People that access or utilize a Document is considered to be the Document Users of such Document. The Document User has the responsibility to comply with this Policy at all times.

Determining the corresponding classification of a particular data allows a unit or office to better protect it and at the same time, allow it to be more accessible to the proper and authorized parties.

Section 4: Retention and Disposal Policy

While there is no hard and fast rule in determining how long data should be retained, every office or unit 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.[10] 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.

However, it must be noted that personal information cannot be retained in perpetuity for a possible future use that is yet to be determined.

[9] Part II. Responsibilities, Revised Data Classification Policy, Memorandum Reference No. EBM 20-06 dated 11 May 2020.
[10] Sec. 11 (e), Chapter III, R.A. No. 10173

Units and offices are enjoined to dispose excessive copies of documents in such a way that the data therein cannot be reconstituted, provided that the following requisites are met:[11]

a. There is no law or regulation requiring the continued use or retention of the document;
b. UP Diliman has no foreseeable indispensable need for the document; and
c. No data subject rights shall be violated.

The following issuances may serve as a guide 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.

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.

Chapter II – System and Data Access and Control Policy

Section 1: Access

In order to ensure that information stored in the various units and offices are protected from unauthorized access, the following guidelines must be observed:

First, entrance to the repositories of personal data should be limited to authorized UP People only. Visitors entering the premises of the building are required to login with the guard-on-duty. They cannot, unless authorized or has obtained the appropriate approval, access the personal data held by the said unit;

Second, physical storage locations such as, but not limited to, folders, filing cabinets, envelope drawers, and other storage devices, when not in use, shall be kept secured and locked;

Third, units and offices with paper-based filing systems must maintain an access log to track the historical access and use of the files that were accessed, as well when, where, why, by whom, and whether copies of the accessed files were made;

[11] Item B (10), Chapter IV. SECURITY MEASURES, UP Diliman Privacy Manual (Data Protection Team Memorandum Reference No. EBM 19-02, dated 11 November 2019).

Fourth, there must at all times be a person responsible and accountable for a storage device containing personal data, whether portable or no. Such person shall at all times ensure the physical and technical security of the storage device and, if practicable, encrypt the device or encrypt the confidential or sensitive confidential information therein;

Fifth, all computer systems must be protected by a strong password or passphrase. Passwords and passphrases should at least be a minimum of twelve (12) characters. The UP Diliman Computer Center shall ensure password and passphrase policies are at par with security best practices. As far as practicable and practicable, a multi-factor authentication method must also be employed. Passwords and passphrases used should comply with the Password/Passphrase Policy found in this document. Computer systems should not be left unattended. If necessary, the respective UP Staff must use a screensaver and with a password in order to prevent any unauthorized access; and

Sixth, all units and offices must be mindful of the parameters set by the UP Diliman Data Classification Policy[12] in determining the classes of users who may have access to the documents and files that they hold.

Section 2: Online Access to Personal Data

Personal data may be accessed physically or online. Due to the fast-paced changes in technology, units and offices must ensure that the personal data they hold is likewise free from unauthorized online access.

Except if there is prior express documented approval by a superior to address and urgent or important need, access to personal data online by UP People must be made only through official devices. These devices must also be protected by a strong password or passphrase. As far as practicable, a multi-factor authentication must be employed. Moreover, access to these devices may only be granted to authorized UP People. Passwords and passphrases used should comply with the Password/Passphrase Policy found in this document.

All systems allowing online access to personal data must likewise have an access log to reflect the proper timestamps of the activities conducted by the account holder pertaining to the personal data.

Preferably, digitally processed personal data, whether in transit or at rest, should be encrypted. Moreover, units and offices are mandated to make use of technologies which prevent personal data accessible online from being copied to a local machine.

Units and offices, together with their Privacy Focal Persons, must have and access control list to define the roles (not persons) that may have online access to personal data.[13]

[12] UP Diliman Data Classification Policy, 2 January 2020 Data Protection Team Memorandum Reference No. EBM 19-03

[13] Chapter IV. SECURITY MEASURES, UP Diliman Privacy Manual (Data Protection Team Memorandum Reference No. EBM 19-02, dated 11 November 2019).

Section 3: Remote Access

Only UP Diliman Officials, Staff and Faculty may access personal data online or remotely. Should an external party request for the disclosure of data, a formal documented request explaining its legitimate purpose must be made through the respective unit or office's Privacy Focal Person.

Reduce, if not entirely, do away with a Bring-Your-Own-Device or BYOD practice wherein employees can work and access data through the use of their own personal devices such as laptops, tablets, or mobile phones. While this practice may seem convenient, it exposes the unit to a number of information security risks. Hence, it is best to remotely access data using devices issued by their respective unit or office. However, should the concerned UP Staff and Faculty be constrained to use his personal devices, it is incumbent upon him to exercise the proper diligence in the use of the same and uphold at all times the privacy and confidentiality of the information being processed prescribed by the UP Diliman Remote Work Privacy Guidelines.[14]

Devices used to access UP Diliman data must be equipped with the appropriate physical and technical security measures.

Remotely accessible Data Processing Systems must be protected by a strong password or passphrase, and if available, a multi-factor authentication system. Passwords and passphrases used should comply with the Password/Passphrase Policy found in this document.

Remote access is allowed using only one's official UP account to access an official cloud service.

Section 4: Remote Disconnection and Wiping

Remote disconnection is a security feature that allows the disconnection of an official device in case an official device used to access and process data is lost or stolen, or when its authorized user or holder ceases to be connected with its unit or office. Remote wiping, on the other hand, is another security feature that allows data to be remotely deleted from an official device in case any of the aforementioned instances should likewise occur. It is strongly recommended that devices are enabled and ready for these features.

In the event of a loss of device or separation of service, such fact shall be reported to the immediate superior, the Privacy Focal Person, and all concerned I.T. Personnel who will immediately act to consider options, with a strong preference for remote disconnection and/or wiping of the device with the approval head of office or unit.

In relation thereto, device users are instructed to regularly backup all data stored in remote devices in a secure and authorized platform.

[14] UP Diliman Remote Work Privacy Guidelines, UPD DPO Memorandum No. EBM 20-04 issued 20 March 2020.

Section 5: Guest Access, Separate Guest Network, Third-Party Connection

In order to prevent unauthorized online access to personal data, units and offices shall, as far as practicable, provide a guest network which may be used by third parties or guests who, if necessary, need to connect their devices to the network of a UP Diliman unit or office.

Use and access to UP Diliman networks are subject to UP's Acceptable Use Policy[15] and related policies.

Section 6: Virtual Private Network (VPN)

Virtual Private Networks should be set up for remote access to UP Diliman network, systems, or servers that, in the determination of the UP Diliman Computer Center[16] or the concerned Privacy Focal Person or I.T. Personnel will pose a medium or a high risk to UP Diliman, its systems, or its information.

Chapter III – Communications and Email Policy

Section 1: Messages and Communications

The creation, sending, transmittal, receipt, access, use, processing, and storage of emails and other electronic messages are governed by the UP Diliman Message and Communications Policy.[17] Pursuant to the this policy, all official emails containing personal, privileged, or confidential information sent to external parties should state a Privacy and Confidentiality Notice.[18] While there is no particular form, the said notice should substantially contain the points in the ***suggested*** notice below:

> Privacy and Confidentiality
>
> This message, its thread, and any attachments are privileged and confidential. No part of this message may be reproduced or exhibited in any form or manner without the consents of the sender and the University of the Philippines Diliman. In case of wrongful receipt of or unauthorized access to this message, please immediately inform the sender and permanently delete all wrongfully received copies. Your access to this message subjects you to the UP Diliman Message and Communication Policy and relevant data privacy regulations.

[15] Accessible at https://upd.edu.ph/aup/
[16] UP Diliman VPN Guidelines https://upd.edu.ph/vpn/
[17] UP Diliman Message and Communication Policy, Office of the Chancellor Memorandum No. MLT 18-135 issued 23 May 2018
[18] Ibid.

The ***suggested*** Filipino version of the notice is as follows:

> Pabatid sa Pribasiya at Pagiging Kumpidensiyal
>
> Ang mensaheng ito, kasama ang mga karugtong, at anumang mga kalakip ay pribado at kumpidensiyal. Maliban sa tunay na layunin ng mensahe, walang bahagi nito o identidad ng tao ang maaaring ibunyag, kopyahin o ipalabas nang walang pahintulot mula sa nagpadala. Kung di-sadyang natanggap o nabasa ang mensaheng ito nang walang pahintulot, agad na ipagbigay-alam sa nagpadala at permanenteng burahin ang lahat ng di-sadyang natanggap na kopya. Ang iyong pag-akses sa mensaheng ito ay nangangahulugang sumasailalim ka sa UP Diliman Message and Communication Policy at anumang kaugnay na mga tuntunin ukol sa pribasiya ng datos.

The notice may be in any language most understood to its recipients.

Section 2: Transfer of Personal Data

All UP People are enjoined to exercise diligence in all their affairs involving the transfer of personal data through all channels. They must, at all times, ensure that the privacy and confidentiality of the personal data is maintained.

The disclosure or transfer of data containing personal data shall be conducted by UP People whose work functions include the disclosure or transfer when related to a legitimate purpose of the concerned UP Diliman unit or office. In case of special circumstances wherein the work functions of the individual involved do not include the disclosure or transfer of data concerned, then the approval of the Privacy Focal Person having jurisdiction is necessary.

Emails

UP Mail (@up.edu.ph) is an email service available to all currently enrolled UP students and employed faculty and staff (whether regular, or contractual or Individual Contract of Service), and offices. UPD Webmail (@upd), including its unit specific subdomains (@xxx.upd.edu.ph), on the other hand is an email service maintained by the UP Diliman Computer Center. The former is used as the official access to the Core Information Systems and standard to all constituent universities (CUs).

The use of the UP Mail, and UPD Webmail and its subdomains, is a privilege granted by the University to the UP People. Thus, the latter have no vested rights over the same.

The use of the University's email services, shall be for official academic or work-related purposes only. It should not be contrary to law, morals, and public policy. The use of one's personal email is strictly prohibited unless there is an important urgent matter and the user has no access to UP Mail and UP Webmail.

In sending emails, UP People are to refrain from including as recipients those who have no official business in the matter. Unnecessary private and confidential information should be redacted. When necessary, a Privacy and Confidentiality Notice footer and/or Sensitive Confidential information should form part of the email.[19]

In addition, the following security guidelines are to be observed:

a. Use of a strong password or passphrase and multi-factor authentication;
b. Exercise constant vigilance in accessing links and downloading attachments. Ensure that the attachment came from a legitimate source. Corollary thereto, refrain from sending emails to unfamiliar recipients;
c. Refrain from accessing links or opening emails from unfamiliar sources. Be wary of phishing or malware attempts;
d. Be cautious of suspicious emails or those containing inconsistencies such as grammar mistakes, excessive punctuation marks, requesting for donations, etc.;
e. Refrain from excessively downloading files. Download only what is necessary;
f. Only the registered account holder can access their corresponding email accounts. Disclosing of login credentials is strictly prohibited;
g. Access to email accounts should be made through secure and private connections only;
h. Ensure that the anti-virus and anti-malware programs are regularly updated; and
i. In the event of a security breach, the account holder should immediately inform the UP Diliman Computer Center.

Any email containing Private Information wrongfully received or accessed without authority should be immediately deleted and disposed of. Moreover, the University and the sender of the Private Information wrongfully received or accessed without authority should immediately be informed.[20]

In order to maintain the professionalism and proper representation of UP Diliman, UP People are highly encouraged to create an email signature in the suggested format:

[Employee Name]

[Designation]

[Academic Unit/Administrative Office]

University of the Philippines Diliman

All users of the abovementioned email services are bound to comply with the Security Measures laid down in the UP Diliman Privacy Manual[21] as well as UP Diliman's Acceptable Use Policy.[22]

[19] UPD DPO Memorandum No. 20-05, UP Diliman Email Policy, 05 May 2020
[20] *See* Note 12
[21] Chapter IV, Data Protection Team Memorandum Reference No. EBM 19-02, dated 11 November 2019
[22] Accessible at https://upd.edu.ph/aup/

Personal Productivity Software

Personal productivity application software refers to various programs that aid individuals to effectively and efficiently perform their tasks.[23] These applications are categorized according to their usage, such as: word processing, spreadsheet software, database management, and presentation.[24]

Briefly, these applications are described as follows:

a. Word processing software are used to produce, edit, format, and print documents.[25] These are used to create or draft memos, letters, reports, and the like.
b. Spreadsheet software or electronic spreadsheets perform calculations on data based on a formula that is entered by a user. The formulas range from simple mathematical (addition, subtraction, division, and multiplication), financial, statistical, and database functions. In addition, the data can be presented through visual representations such as graphs or charts.[26]
c. Database management software allows users to create, access, and manage a database.[27]
d. Presentation software allows users to create a visual representation of data through text, graphics, animations and sound.

Personal productivity applications are indispensable in the performance of ones official functions in their respective unit or office. However, UP People are prohibited from using, installing, or creating an illegal copy of the software application.

UP Student, Staff and Faculty can avail Personal Productivity Software thru UP Information Technology Development Center.[28]

Portable Media

Preferably and as much as practicable, the saving of files to portable storage devices (such as external hard disks, USB flash disks and optical disks) should be prohibited by UP Diliman units and offices. Drives and USB ports on local machines may also be disabled as a security measure. An allocated network drive shall always be preferred to saving files locally to a machine. In case there is a need to save in a local machine or a portable storage device, only UP People and not external parties may access such files. If there is a need to save files in portable storage devices, only official portable devices encrypted with technologies not falling below industry standards shall be used with the consent of the concerned Privacy Focal Person.

Portable media are devices that can be inserted an removed from a system, such as a computer, used to store information.[29] The use of portable media exposes units or offices to possible data loss in case the device is lost, stolen, or the data therein is exposed to a third party.

---

[23] https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/productivity-software
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] http://itlibrarian.com/module04/
[28] Follow the guidelines in https://itdc.up.edu.ph/uis/microsoft-office-365-for-up
[29] "portable storage device" as defined by the Computer Security Resource Center of the United States' National Institute of Science and Commerce, https://csrc.nist.gov/glossary/term/portable-storage-device

Units and offices using portable media to store personal data must ensure that the devices used are owned by UP Diliman and shall be strictly for official use only. Moreover, it is necessary that the data stored therein are encrypted.[30] Laptops used by the units and offices in the performance of their respective duties and functions must also be encrypted[31] and password/passphrase protected.

As a general rule, the manual transfer of personal data stored in removable devices, such as USB flash drives, shall not be allowed. However, if the mode of transfer is necessary or unavoidable, authentication technology such as one-time PINs, or passwords, should be employed.[32]

In order to avoid malicious attacks infiltrating the computer system where the device will be connected, the same must first be scanned and the computer system should likewise have an updated system security software.

In the event that the portable media is lost, stolen, or its holder has ceased to be connected to the office or unit, the matter must be brought to the attention of the unit or office's Privacy Focal Person who shall request for the remote disconnection and/or wiping of the device, when applicable.[33]

Fax Machines

Due to the lack of technical security measures to safeguard the transfer of data, such as encryption and authentication processes, facsimile or fax machines shall generally not be used to transmit documents containing personal data.[34] In exceptional cases that it is absolutely necessary to transfer data through facsimile, then the prior approval of the immediate superior shall be documented. In no case shall sensitive personal information shall be transmitted through facsimile.

Section 3: Email Management – Archiving and Deletion

Emails containing personal data may be archived pursuant to the rules provided by the National Archives of the Philippines Act of 1997,[35] provided they are of enduring value.[36]

Wrongfully received emails must be verified if indeed wrongfully received and must be permanently deleted upon verification of the fact of wrongful receipt. The incident must likewise be reported to the sender.[37]

[30] Sec. 26, Rule IV, NPC Circular No. 16-10, dated 10 October 2016.
[31] Ibid.
[32] Ibid., Sec. 27, Rule IV.
[33] See Chapter II, Section 4 of this Policy.
[34] Sec. 28, Rule IV, NPC Circular No. 16-10, dated 10 October 2016.
[35] Republic Act No. 9470
[36] Sec. 30, Rule IV, NPC Circular No. 16-10, dated October 2016.
[37] 23 May 2018 Office of the Chancellor Memorandum No. MLT 18-135

Chapter IV – Website and Cookie Policy

The Data Privacy Act emphasizes the need for transparency in the processing of personal data. Therefore, users of a website must be informed if their personal data is being processed, and if so, the nature, extent, and purpose thereof.[38]

If a unit or office's website collects personal data and/or uses cookies, then their website should include a privacy notice.[39]

Cookies are blocks of data that are used to ease the navigation through a website.[40] Despite being functional, cookies also expose the user to possible information security risks because they also serve as means to identify the user and his activity in the site. Eventually, the website owner will be able to determine the user's browsing habits, often without the latter's consent.[41]

The UP Diliman Website[42] uses cookies to prevent security risks, recognize that the user is logged in, customize the user's browsing experience, store authorization tokens, permit social media sharing, troubleshoot issues, and monitor anonymized or aggregated statistics.[43] In line with the National Privacy Commission's requirement, all UP Diliman websites must have a Privacy Notice if personal data is collected or if cookies are used.[44]

Chapter V – Acceptable Use Policy

The use of the DILNET, WiFi@UPD, UP VOIP, UP VPNs, and other information technology resources in or from UP is subject to the Acceptable Use Policy[45] of Information Technology Resources of the University of the Philippines System. The Policy aims to provide a set of rules and regulations to govern the use of the computing facilities, networks and other information technology resources of the UP System. These rules were crafted in order to guarantee the equitable, safe, and reliable use of the said resources.

---

[38] National Privacy Commission Privacy Policy Office Advisory Opinion No. 2017-47, dated 29 August 2017.
[39] NPC Privacy Tool Kit, 3rd Edition
[40] Ibid.
[41] Ibid.
[42] https://upd.edu.ph/
[43] General Privacy Notice

x x x x

1. Acts of Processing

x x x x

The UP Diliman Website uses cookies to prevent security risks, recognize that the user is logged in, customize the user's browsing experience, store authorization tokens, permit social media sharing, troubleshoot issues, and monitor anonymized or aggregated statistics. (https://upd.edu.ph/privacy/notice/)

[44] Section 65, Data Privacy Act Implementing Rules and Regulations
[45] See Note 15.

Chapter VI – Password/Passphrase Policy

It is a must for all UP People to employ a strong password or passphrase to protect their respective devices from unauthorized use or access of email and email-enabled systems.

A password is a string of characters, usually comprised of letters, numbers, and other symbols, that are used to authenticate the identity of a particular user or verify one's access authorization.[46]

A passphrase is a sequence of words or text that, similar to a password, a user employs to authenticate his identity. For security purposes, it is generally longer than passwords but are easier to remember.[47] It must be difficult to guess, therefore, words or phrases that may be remembered by the user. Common famous names or phrases should not be used.

Weak or poor choice of password or passphrase, using the same password for all devices or services, and sharing one's password to others are only few of the many ways others tend to expose their organization to information security risks.

In crafting a strong password or passphrase, it must be both easy for the user to remember but difficult to be figured out by others. Often, websites or services require their users to come up with a password of at least a particular length with varied alphanumeric characters. It should not be based on the user's personal information, favorites, names of relatives or pets, or other any piece of information that may be easily guessed, or common patters. Passwords and passphrases should at least be a minimum of twelve (12) characters.

Examples of weak passwords:

- 12345
- Asdfghjkl

Examples of strong passwords:

- YouN33dCapital
- Refreeg1rat0r

Examples of weak passphrases:

- HelloThere
- LuckyMe

Examples of strong passphrases are:

- LeBronJamesBondPaper
- HairyPotterAndThePilosopoStoned

[46] United States' National Institute of Standards and Technology Special Publication No. 800-12, June 2017, https://doi.org/10.6028/NIST.SP.800-12r1.
[47] United States' National Institute of Standards and Technology Special Publication No. 800-63-3, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

When mandated by the UP Diliman Computer Center or the UP Diliman Data Protection Office for a device, system or service, multi-factor authentication should be enabled.

Chapter VII – Backup Policy

To back up information is to create multiple copies of the same in order to facilitate its recovery if necessary.[48] In the event of a data breach or incident, units and offices are expected to have a procedure to recover and restore the data and continue its operations. Thus, it is necessary for every unit or office to back up the personal information that they hold.

Section 1: What to back up

Units and offices are required to maintain a backup file for all the personal data it holds. Files that have been changed or modified must also be backed up regularly.

It must be noted that while a full backup may be time consuming, it saves all the files and provides the fastest recovery method.

Section 2: How to back up

Storing a unit or office's personal data in a single back up drive is not sufficient. As much as possible, units and offices are strongly enjoined to back up their data in three different platforms or storages that are not stored in a single location.

The units or offices must also endure that all employed backup facilities are equipped with the appropriate security measures (e.g., encryption) to protect the stored data.

Section 3: Data Recovery Capability

It is highly advised that regular testing, assessment, and evaluation be conducted to check whether the back up systems employed by the units and offices can effectively and timely save the data as well as retrieve and restore the same. These checks are also necessary in order to ensure that the data recovered through backup is not inconsistent with the original file.

[48] United States' National Institute of Standards and Technology Special Publication No. 800-34, May 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Chapter VIII – Technical Incident Response and Reporting Policy

The UP Diliman Computer Center issued a Network and System Security Checklist,[49] which lays down the Computer Center's security policy and how incidents, depending on the situation are handled.

The UP Diliman Computer Center shall determine if a system affected by a technical incident should be subjected to a Vulnerability Assessment and Penetration Testing. Concerned Privacy Focal Persons shall remediate gaps found by any assessment, testing or audit of a system.

Chapter IX – Personal Data Breach Management

Section 1: Security Incident Management Policy

The UP Diliman Data Privacy Security Incident Management Policy (Office of the Chancellor Administrative Order No. MLT-19-072)[50] established the procedure to prepare for, manage, and recover from privacy security incidents and personal data breaches. The policy provides implementing details to monitor, mitigate, investigate, respond to, contain, report, and resolve security incidents and personal data breaches.

Section 2: Threats, Risks, and Vulnerabilities

Threat refers to "a potential cause of an unwanted incident which may result in harm to a data subject, system, or organization". A threat may trigger or exploit a vulnerability.[51]

A risk, on the other hand is "the potential of an incident to result in harm or danger to a data subject or organization".[52]

A vulnerability is a "weakness of a data processing system that makes it susceptible to threats".[53]

Every data processing activity has a corresponding risk. While it may be extremely difficult to eliminate it, risks can be managed to minimized in order to ensure the security of personal data in UP Diliman.

---

[49] https://upd.edu.ph/wp-content/uploads/2019/03/UPD-Security-Checklist.pdf
[50] https://upd.edu.ph/wp-content/uploads/2019/04/Data-Privacy-Security-Incident-Management-Policy.pdf
[51] Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication No. 800-30, July 2002 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf
[52] NPC Privacy Tool Kit, 3rd edition,
[53] 31 July 2017 NPC Circular No. 17-01 defines a data processing system as "a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing."

Depending on organizational or operational needs, risk may be computed through any of the following:

Risk = Threat x Vulnerability

or

Risk = Threat x Vulnerability x Impact

or

Risk = Threat x Vulnerability x Probability

or

Risk = Threat x Vulnerability x Impact x Probability

A risk heat map may be devised to determine risk levels of various facets of operations.

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 possibly of resulting to a risk. This series of activities include[54]:

a. *First*, identify or assess the data processing activities and systems of a unit;

b. *Second*, identify the possible threats that may trigger or exploit the weaknesses of the data processing activities and systems of a unit. In identifying these threats, one must consider all the possible sources (natural, human, and environmental). Once the possible sources are identified, their corresponding threat actions should be determined.
   Threat actions are the methods that are used by threat sources to carry out an attack.
   e.g., Threat source: Hacker;
   Threat action: hacking

c. *Third*, identify the possible vulnerabilities or weaknesses in the data processing activities or systems of the unit. The identified flaws or weaknesses can then be paired to their corresponding potential threat and threat actions
   e.g., Vulnerability: Weak password/passphrase system
   Threat source: Employee
   Threat action: Login credentials are exposed in the workstation

d. *Fourth*, analyze the controls that are being used or planned to be used in the unit in order to secure the data processing activities or system that may minimize the likelihood of a threat exploiting a vulnerability.

[54] Adopted from Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication No. 800-30, July 2002
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

e.g., Vulnerability: Weak password/passphrase system
Threat source: Employee
Threat action: Login credentials are not regularly updated (default password still in use)
Control: Personnel guidelines that may include requiring members of the unit to periodically update their passwords

Through these activities, units and offices will be able to identify the possible threats to their activities and systems' weaknesses, and in turn, formulate additional controls that may strengthen them.

In addition, units and offices are highly enjoined to participate in the Privacy Impact Assessment (PIA) conducted by the UP Diliman Data Protection Office. This activity determines how personal information is being processed, including the privacy risks that may be involved and how to manage the same.

Section 3: Data Breach Response Team

UP Diliman teams that are mandated to assess and evaluate security incidents, including personal data breaches, restore integrity to the information and communication system, mitigate and remedy resulting damages, and comply with reportorial requirements are called Data Breach Response Teams (BRTs).[55]

Under the Data Privacy Security Incident Management Policy,[56] UP Diliman has a Constituent University-level BRT known as "Diliman-Level BRT" while every academic unit and administrative office is required to establish its own BRT known as the "Unit-level BRT". These BRTs are under the jurisdiction and authority of the UP Diliman Data Protection Officer.

The Diliman-level BRT is composed of the following members:

a. UP Diliman Data Protection Officer as Chair;
b. Director of the Computer Center as Deputy Chair;
c. A representative from the School of Library and Information Studies (SLIS);
d. A representative from the Human Resource Development Office (HRDO);
e. A representative from the Office of the University Registrar (OUR); and
f. A representative from the Diliman Legal Office (DLO)

If a security incident[57] involves the personal data of a student, parent, or guardian, then the PFP of the Office of Vice Chancellor for Student Affairs shall *motu proprio* become a support and resource person of the Diliman-level BRT.

[55] Administrative Order No. MLT 19-072, Data Privacy Security Incident Management Policy, dated 25 March 2019
[56] Ibid
[57] Administrative Order No. MLT 19-072 defines a *security incident* as an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It also defines the term *personal data breach* as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

If a security incident involves personal data processed by an office under the Office of the Vice Chancellor for Administration (OVCA), then the PFP of the OVCA shall *motu prorpio* become a support person for the Diliman-level BRT.

If a security incident involves personal data handled by an alumnus, then the PFP of the academic unit of the alumnus shall *motu proprio* become a support and resource person of the Diliman-level BRT.

The Unit-level BRT, on the other hand, shall be composed of the following:

a. The unit or office's PFP, who shall have the authority to decide on privacy-related matters in case of a personal data breach. The PFP shall serve as the leader and coordinator of the Unit-level BRT;
b. An officer of the UP Diliman Unit or office with the authority to decide on relevant administrative matters in case there is a data breach;
c. A Data Processor or information security person with knowledge how personal data is being processed by the unit or office.

For every Privacy Concern[58],the PFP shall coordinate the monitoring, mitigation, investigation, response, containment, reporting, and its unit's contribution to resolving the privacy concern.

Both the Diliman-level BRT and Unit-level BRTs are under the jurisdiction and authority of the UP Diliman Data Protection Officer.

Chapter X – Wireless Policy and Network Security Policy

Section 1: Network Security Policy

All users of the UP Diliman Information Technology System (IT System)[59] are responsible for preserving the integrity and security of its resources, including the information in transit through its networks.

Thus, UP People are strongly enjoined to practice the appropriate Security Measures prescribed in the UP Diliman Privacy Manual[60] and the Acceptable Use Policy.

Only authorized UP People are allowed to manage and make changes in the network and network infrastructure devices. Moreover, any change or modification must be subject to the approval of

[58] *Privacy concern*, under MLT No. 19-072, refers to an inquiry, issue, risk, incident, breach, or request referred to the UP Diliman PFP having jurisdiction over the relevant UP Unit.
[59] Refers to the includes computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, and software, databases and other data files that are owned, managed, or maintained by any unit of the University of the Philippines.
[60] See Note 14

the appropriate office (i.e., UP Diliman Computer Center), and in accordance with its established guidelines, if any.

Remote access to UP Diliman's network shall be controlled and managed by the UP Diliman Computer Center. The latter may, when appropriate, establish guidelines in establishing a secure access to UP Diliman's network such as, but not limited to, the use of a DilNet Account.

System privileges and access permissions in performing system management functions must be strictly logged. These logs must be subject to regular monitoring and audit.[61]

The UP Diliman Data Protection Office shall closely coordinate with the UP Diliman Computer Center for the regular testing, assessment, and evaluation of the security of the University's network.

Section 2: Wireless Policy

All devices such as, but not limited to, mobile phones, tablets, laptops, and computers, connecting to the UP Diliman access points (Dilnet and WiFi@UPD) shall be subject to the Acceptable Use Policy for Information Technology Resources of the UP System. UP People using the wireless access points within UP Diliman are likewise enjoined to practice the Security Measures laid down in the UP Diliman Data Privacy Manual.[62]

Furthermore, UP People using the said devices are strictly prohibited from interfering with the configuration of the wireless network, unless authorized.

Moreover, in order to secure the computer assets and data processing systems of units and offices, UP People shall only access data and information through secure network connections. In connecting to DilNet WiFi or other hotspots, it is a rule of thumb to determine whether the same is a secured and a legitimate network.

Chapter XI – Encryption Policy

Encryption involves the transformation of data, through the use of code keys, into a form that conceals its original meaning to prevent unauthorized access or use.[63] In order to be properly read by the authorized parties, the transformation must be reversed (decryption) and the information must be restored to its original state.[64] This is also done through the use of code keys.

The National Privacy Commission requires that personal data digitally processed by government agencies, including SUCs such as UP Diliman, must be encrypted, whether at rest or in transit.[65]

---

[61] https://www.librariesni.org.uk/AboutUs/OurOrg/Policies%20and%20Procedures/Network%20Security%20Policy.pdf
[62] See Note 14
[63] "encryption" as defined by the International Association of Privacy Professionals (IAPP) (https://iapp.org/resources/glossary/#e-authentication-2)
[64] United States' National Institute of Standards Technology Special Publication No. 800-82, May 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[65] Sec. 8, Rule II, NPC Circular No. 16-01, dated 10 October 2016.

Section 1: Encryption Standard

Personal data in rest, in transit and in use must at all times maintain their confidentiality, integrity and availability through compliance with this Policy, the implementation of which should be led by Privacy Focal Persons.

The National Privacy Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) for the encryption of all digitally processed data, whether at rest or in transit.[66]

Personal data that are digitally processed are preferably encrypted, whether at rest or in transit. An appropriate encryption minimum standard (such as Advanced Encryption Standard with a key size of 256 bits (AES-256) or its predecessor technology) is preferred. Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. Passwords and passphrases should at least be a minimum of twelve (12) characters. Passwords and passphrases used should comply with the Password/Passphrase Policy found in this document. The UP Diliman Computer Center shall ensure password and passphrase policies are at par with security best practices.

Section 2: Encryption of Computing Assets

The Staff and Faculty of various units and offices are required to secure the information stored in their unit or office's computing devices using the recommended Advanced Encryption Standard set by the National Privacy Commission. This is to mitigate the risk of unauthorized access or disclosure of data processed or stored in UP Diliman's computing assets. Generally, when a device can be encrypted and recovery keys are available to UP Diliman, or its Computer Center, device encryption should be applied.

UP Diliman issued devices such as laptops and desktop computers, shall be encrypted using the Advanced Encryption Standard set by the National Privacy Commission (AES-256). Other portable devices, when possible and practicable, should likewise be encrypted.

Mobile phones and tablets, whether UP Diliman -issued or personally owned, must also be encrypted. Personally owned laptops, however, need not necessarily be encrypted with the assistance of the UP Diliman Computer Center. *Provided,* however, that no personal or confidential information pertaining to the University or UP People should be stored or processed therein. Furthermore, its use shall be subject to the Security Measures provided in the UP Diliman Privacy Manual[67] and might be subject to the UP Diliman Remote Work Privacy Guidelines[68].

[66] Ibid.
[67] See Note 14
[68] UP Diliman Remote Work Privacy Guidelines, UPD DPO Memorandum No. EBM 20-04 issued 20 March 2020

Section 3: Encryption of Personal Information

Units and offices processing personal information are mandated to secure the personal using the recommended Advanced Encryption Standard set by the National Privacy Commission (AES-256).

Personal information, regardless whether confidential or sensitive, shall only be created, stored, or processed in secure and encrypted computing assets.

In order to protect personal information from interception or unauthorized access. When sending or receiving information, UP People must ensure that it is transmitted through a secure network service. A secure network often requires multi-factor authentication.

In storing personal information, storage devices must likewise be encrypted.[69] In case there is a need to store information in a public cloud based storage, the data must first be encrypted to prevent the facility from possibly decrypting the data.

In the event that a data processing agreement is entered into with a third-party, UP Diliman must ensure that the former likewise employs the appropriate security measures[70] to protect the data, including its encryption.

[69] See Section 2 on Encryption of Computing Assets
[70] See Note 14

Chapter XII – Storage Device Policy, Mobile Device Policy, Bring Your Own Device (BYOD) Policy, Cloud Policy

Section 1: Storage Device Policy

Each external and portable storage device must be under the responsibility of a specific person who shall track its whereabouts and functionality at all times. This person responsible shall be accountable in case the storage device or its contents are lost or unintentionally disclosed.

All UP People are responsible for the safety of the storage devices under their unit or office's care and custody. Portable storage devices are compact and hence may be easily misplaced, or worse, stolen. Therefore, UP People are required to store these devices in a secured location. Moreover, in order to prevent the complete loss of data stored in these devices in case the same are lost or stolen, it is incumbent upon the holders of the devices to regularly back up its contents.

Storage devices are also susceptible to unauthorized use or access. In order to avoid this, UP People must not lend devices to others since it is easy for anyone to steal its contents and even surreptitiously, or even unwittingly, install malicious programs therein and in turn also affect the computer system connected to these devices.

In processing personal information in their respective units or offices, all Staff and Faculty are required to use only UP Diliman issued devices. These official devices shall be for official use only.

At all times, all UP People must ensure that their storage devices containing sensitive personal information, as far as practicable, be encrypted with the recommended Advanced Encryption Standard.

Section 2: Mobile Device Policy

All UP Diliman Staff and Faculty are strictly prohibited from using their personal mobile devices to store, access, or process, the personal information that their respective units or offices process. Furthermore, they must ensure at all times that the mobile devices issued to them by UP Diliman must be for official use only.

In the event of loss, the responsible Staff and Faculty must immediately inform their Privacy Focal Person in order to commence the remote wiping process through the UP Diliman Computer Center.

All UP People are expected to exercise diligence in the use of their mobile devices. They are to exercise caution when accessing links from numbers or addresses that they are not familiar with. As far as practicable, a security software must be installed in their own devices. Moreover, they are enjoined to refrain from storing any personal data processed by UP units or offices unless authorized by the latter.

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 be immediately be permanently deleted permanently from the personal device.[71]

At all times during a work-related file is locally saved in a personal device, external parties are must be prohibited from accessing the personal device.[72]

If appropriate under the circumstances, mobile device users are highly encouraged to regularly backup their devices to prevent any loss of data.

Section 3: Cloud Policy

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. Passwords and passphrases used should comply with the Password/Passphrase Policy found in this document.

UP People must ensure that at all times legitimate cloud storages are used and vigilance should be observed to prevent unauthorized or malicious software such as phishing sites.

Chapter XIII – Firewalls, Antivirus, Intrusion Detection System, OS Patches, Penetration Testing

Section 1: Inventory of Authorized and Unauthorized Devices

Only UP Diliman issued devices shall be used to process personal data processed by a unit or office.

It is incumbent upon every unit or office to regularly conduct an inventory of devices that are used to process the personal data that they handle. This includes not only the computer workstations of every Staff and Faculty but also the portable devices such as, but not limited to, USB flash or hard drives, mobile devices, and laptops. This is to determine whether there are any unauthorized devices that are connected or can connect to the unit or office's system.

Ensuring that only official devices are used in a unit or office reduces the systems vulnerability to attacks.

[71] Sec. 3 UP Diliman Remote Work Privacy Guidelines, UPD DPO Memorandum No. EBM 20-04 issued 20 March 2020.
[72] Ibid.

Section 2: Standard Configurations for Hardware and Software on Laptops, Workstations and Servers

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 hardware of the latter's official devices.

Chapter XIV – Recognition of Electronic Documents and Electronic Signatures; Handling of Electronic Evidence

Section 1: Recognition of Electronic Documents

Subject to policies to be promulgated by the University, UP Diliman shall not turn a blind eye to the legitimacy of actions and decisions by the fact that they are embodied in electronic documents or signed either electronically or digitally. Documents shall not be discriminated against by the fact that they are electronic. Subject to policies, electronic documents and signatures shall have the legal effect, validity, and enforceability as any other document or legal writing.[73]

When a document is required by law to be in writing, this requirement is satisfied by an electronic document if its integrity and reliability is maintained, and it is capable of being authenticated. In determining the integrity and of an electronic document, the following criteria must be satisfied: *First*, the determination of the completeness of the document. *Second*, the determination that the information in the document is unaltered. The reliability of the document is determined depending on the purpose for which the information was generated and other surrounding circumstances.[74]

---

[73] Sec. 7, Chap. II, Republic Act No. 8792

[74] Section 7. *Legal Recognition of Electronic Documents* - Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and -

(a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that -

i. The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and

ii. The electronic document is reliable in the light of the purpose for which it was generated and in the light of all relevant circumstances.

(b) Paragraph (a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the document not being presented or retained in its original from.

x x x x

Section 10. *Original Documents.* -

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if;

(a) the integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence aliunde or otherwise; and

(b) where it is required that information be resented, that the information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purpose of subparagraph (a) of paragraph (1):

Section 2: Recognition of Electronic Signatures

Subject to policies to be promulgated, UP Diliman shall not discriminate against and recognize that an electronic signature on an electronic document is equivalent to the signature of a person on a written document if it is proved that it was not altered by any of the parties interested in the electronic document.[75]

Electronic signatures on an electronic document are presumed to be the signature of the person to whom it relates and it was affixed therein with the intention to sign or approve the said document.[76] Digital signatures (which are asymmetrically encrypted electronic signatures) from the Philippine National Public Key Infrastructure (PNPKI) shall not be discriminated against.[77]

Section 3: Handling of Electronic Evidence

The offer or use in evidence of electronic documents and electronic data messages in administrative cases shall be subject to the Rules on Electronic Evidence or its successor rules as promulgated by the Supreme Court.[78]

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display ; and
(b) the standard of reliability required shall be assessed in the light of purposed for which the information was generated and in the light of all the relevant circumstances.

[75] Ibid., Sec. 8
[76] Ibid., Sec. 9
[77] To apply for Electronic Signature, see Guidelines on online application for digital signature, DPO Advisory Reference No. EBM 20-002 dated 11 May 2020.
[78] Sec. 2, Rule I, Rules on Electronic Evidence, A.M. No. 01-7-01-SC, July 17, 2001