UP Provident Fund Inc.

Information Securtity Policy

Roy Vincent L. Canseco (c) 2020 Manila

Revision 0.1
06.2020

Table of Contents

```
This is draft version 0.1
```

1

Introduction

1.1. Objective

The objectives of this document are to:

- Describe measures to protect information and information systems in UP Provident Fund Inc.
- Promote confidentiality and integrity while keeping the availability of UPPFI's information and data.

1.2. Scope

This policy pertains to the processing of all data and information flowing to, within and out of UPPFI as well as all information and computer systems used controlled or owned by UPPFI, including hardware, software and their connectivity.

1.3. 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 signature refers to any distinctive mark, characteristics and/or sound in electronic form 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;

4. Personal Data refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;

2

Data Governance, Management and Retention Policy

2.1. Data Inventory

Data Inventory is a preliminary step in conducting a Privacy Impact Assessment. In this process, the office identifies the following

- the different personal data it collects,
- its source,
- its destinations,
- its storage,
- and the roles/ persons responsible and accountable for the information.

2.2. Data Stewardship

To effectively comply with the Data Privacy Act of 2012 (DPA 0f 2012), UPPFI can identify a **Data Protection Team** comprised of the following:

1. A member of the Board or its representative
2. The head of operations or his/ her representative
3. The head of I.T. or his/her representative
4. Other personnel as the case warrants

The teams is to answer directly to the UPPFI Director regarding data protection matters. The Director, as representative of UPPFI acknowledges the role of

personal information controller (PIC), and would designate from the Data Protection Team a leader, known as the Data Protection Officer (DPO). As UPPFI has multiple offices, Privacy Focal Persons (PFP) are to be assigned per office. PFP's shall assist the DPO and Data Protection Team to coordinate, cascade and apply the rules and regulations pertaining to the Data Privacy Act as well as all pertinent laws and issuances.

2.3. Data Classification

Documents in UPPFI are classified in terms of their availability:

- Public or
- Restricted.
- Internal Data
- Confidential Data

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

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

First, Internal data should be internally contained within UPPFI offices. It may be accessed 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 or reputational risks. It is given on a need-to-know basis.

Awareness of the classification of a particular document allows the office to better protect it while keeping it accessible.

2.4. Retention and Disposal Policy

Data should be retained only for as long as it is necessary for the legitimate purpose for which the data were collected.

Personal information should NOT be retained in perpetuity for a possible future use that is yet to be determined.

Offices are enjoined to dispose excessive copies of documents in such a way that the data therein cannot be reconstituted

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; and
4. Executive Order No. 2, series of 2016 on Freedom of Information and subsequent related executive orders and laws

3

System and Data Access and Control Policy

3.1. Access

These are the guidelines to prevent unauthorized access of information:

Guidelines against unauthorized access

1. Non-UPPFI personnel may not access personal data held by the office without appropriate approval.
2. Physical storage locations such as filing cabinets shall be secured.
3. For paper-based systems, a logbook of historical access shall be maintained. The logbook shall contain who accessed what, when, and for what purpose.
4. Staff and officers are to be responsible and accountable for storage devices containing personal data, whether personal or not. Encryption is recommended whenever practicable, with considerations to business continuity.
5. Computer systems are to be protected by strong passwords / passphrases. Computers are to auto-lock when left unattended for a reasonable amount of time. Multi-factor authentitcation should be considered when practical.

6. Offices are to consicously put down mechanisms that use data and documents in a manner that is aligned with their classifications. For example all internal documents should not leave the office as much as possible. All confidential documents should be in sealable envelopes.

3.2. Online Access to Personal Data

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.

For electronic transit of data, it shall be using encrypted links such as Secure Sockets Layer (SSL) as digital certificates.

Encrypting of data at rest/ storage is to be considered if practical with respect to business continuity.

3.3. Remote Access

Remote access to UPPFI software platforms must be through UPPFI accounts, whether member ID numbers or official employee email addresses. No random usernames shall be used.

3.4. Remote Disconnection and Wiping

To limit the need for disconnection and wiping, UPPFI shall use cloud-based platforms.

Official emails by employees will be done through the provided UPPFI emails. Communication through mobile phones will use voice calls. Passwords are to be changed once suspected to be compormised. Employee accounts will be deactivated as part of any resignation or retrenchment process.

3.5. 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.

Heads of each office shall determine Acceptable Use Policies for guest internet networks.

3.6. Virtual Private Network (VPN)

To limit the need for Virtual private networks, we utilize UPPFI-provided and controlled cloud-based file storage platforms such as One Drive, Google Drive, Dropbox or OwnCloud.

4

Communications and Email Policy

4.1. Messages and Communications

Official employee emails should have a Privacy and Confidentiality notice that more or less looks like the following:

> **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.

Alternatively, we can adapt a Filipino notice that is more or less like the following.

> **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.

Any language, as long as it is understood by recipients, is fine.

4.2. Transfer of Personal Data

Any employee handling a transfer of personal data NOT directly related to his/her role, must inform the Privacy Focal Person in his/her office of the DPO or a member of the Data Protection Team in order to be guided in the secure transfer of personal data.

4.2.1. Emails

The use of the UPPFI 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 UPPFI email.

Every employee will be oriented with proper use of the official email. The orientation will be given by the Privary Focal Person, the DPO or anyone from the Data Protection Team.

The orientation will loosely contain the following guidelines.

Email Guidelines

a. Use of a strong password or passphrase or 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 UPPFI Data Protection Team.

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

- Employee Name
- Designation
- UPPFI Office

4.2.2. Personal Productivity Software

UPPFI employees and staff are prohibited from using, installing, or creating a illegal copies of software applications.

4.2.3. Portable Media

As a general rule, the manual transfer of personal data stored in removable devices, such as USB flash drives, shall NOT be allowed.

Instead use the UPPFI email or the office cloud storage.

However, if the mode of transfer is necessary or unavoidable, authentication technology, file storage encryption and passwords, should be employed.

4.2.4. 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.

4.3. 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,[1] provided they are of enduring value.[2]

The email account, and all emails therein are to be deleted after 1 year of the employee leaving UPPFI unless the Data Protection Team has explicitly decided against the deletion of emails/ email account.

[1] Sec. 28, Rule IV, NPC Circular No. 16-10, dated 10 October 2016.
[2] Sec. 30, Rule IV, NPC Circular No. 16-10, dated October 2016.

5

Website and Cookie Policy

The UPPFI Portal[1] 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 and troubleshoot issues. All production (i.e. non-beta) UPPFI websites must have a Privacy Notice.[2] This is in line with the National Privacy Commission's requirement for when personal data is collected or if cookies are used.[3]

[1] http://member.upprovidentfund.com/login

[2] This UPPFI 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.

[3] Section 65, Data Privacy Act Implementing Rules and Regulations

6

Acceptable User Policy

UPPFI offices shall establish an Acceptable Use Policy of Information Technology Resources. The Policy shall provide a set of rules and regulations to govern the use of the computing facilities, networks and other information technology resources of the UPPFI. These rules shall be crafted in order to guarantee the equitable, safe, and reliable use of the said resources.

7

Password/ Passphrase Policy

It is a must for all UPPFI employees and members to employ a good password or passphrase that they will easily remember and others will find hard to guess. For security purposes, it is generally longer than passwords but are easier to remember.[1] This is to protect their respective devices from unauthorized use or access of email and email-enabled systems.

Password/ Passphrase Examples

Examples of weak passwords:

- 12345
- Asdfghjkl

Examples of strong passwords:

- YouN33dCapital
- Refreeg1rat0r

Examples of weak passphrases:

- HelloThere
- LuckyMe

Examples of strong passphrases are:

[1] 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.

> - LeBronJamesBondPaper
> - HairyPotterAndThePilosopoStoned

Whenever practicable, multi-factor authentication should be considered.

8

Backup Policy

8.1. What to Backup

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.

8.2. How to Backup

As much as possible, units and offices are strongly enjoined to back up their data in multiple platforms or storages that are not stored in a single location. Encryption expected in backups unless the Data Protection Team determines otherwise.

8.3. 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.

9

Technical Incident Response and Reporting Policy

UPPFI should put together a Network and System Security Checklist to describe how technical incidents, depending on the situation are handled. The UP Diliman System Security Checklist[1] can be referenced.

[1] https://upd.edu.ph/wp-content/uploads/2019/03/UPD-Security-Checklist.pdf

10

Personal Data Breach Management

10.1. Securing Incident Management Policy

UPPFI should put together a Security Incident Management Policy to provide implementing details to monitor, mitigate, investigate, respond to, contain, report, and resolve security incidents and personal data breaches. The UP Diliman Data Privacy Security Incident Management Policy[1] can be referenced.

10.2. 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.[2]

A risk, on the other hand is “the potential of an incident to result in harm or danger to a data subject or organization”.[3]

A vulnerability is a “weakness of a data processing system that makes it susceptible to threats”.[4]

[1] https://upd.edu.ph/wp-content/uploads/2019/04/Data-Privacy-Security-Incident-Management-Policy.pdf

[2] 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

[3] NPC Privacy Tool Kit, 3rd edition

[4] 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

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
```

The performance of a series of risk assessment would look like the following.

Example Risk Assessment

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

10.3. Data Breach Response Team

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).

communications system or relevant filing system, including the purpose and intended output of the processing."

UPPFI should designate the Data Protection Team as the official BRT.

11

Wireless Policy and Network Security Policy

11.1. Network Security Policy

Changes to the network and network infrastructure are to be according to guidelines.

In the absence of guidelines only authorized UPPFI personnel 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 the Privacy Focal Person or the DPO or a member of the Data Protection Team.

As for the cloud-based system, privileges and access permissions in performing system management functions must be strictly logged.

11.2. Wireless Policy

All devices such as, but not limited to, mobile phones, tablets, laptops, and computers, connecting to the UPPFI access points shall be subject to the Acceptable Use Policy for Information Technology Resources of UPPFI.

12

Encryption Policy

12.1. Encryption Standard

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.

Passwords and passphrases used should comply with the Chapter 7, *Password/ Passphrase Policy* found in this document.

12.2. Encryption of Computing Assets

The Staff and Employees of various offices should secure the information stored in their office's computing devices using the recommended Advanced Encryption Standard set by the National Privacy Commission if they are going to use those computing devices containing member/ employee personal information in a work-from-home or remote work environment or other out-of-office setting.

12.3. Encription of Personal Information

Personal information, regardless whether confidential or sensitive, shall only be created, stored, or processed in secure and encrypted computing assets when working outside of the physical office.

In order to protect personal information from interception or unauthorized access. When sending or receiving information, UPPFI must ensure that communications with its server is transmitted through https, ssh, or a similar encrypted transmission.

13

Device Policies

13.1. 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.

13.2. Mobile Device Policy

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, UPPFI Employees should 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.

13.3. Cloud Policy

Only official UPPFI cloud storages may be used for private or confidential information. Cloud users should undertake the appropriate security measures to protect their accounts.

UPPFI employees 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.

14

Security Policies

14.1. Inventory of Authorized and Unauthorized Devices

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

Regular inventories of devices used for personal data processing should be done.

14.2. Standard Configurations for Different Computers

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

UPPFI devices should have a set of standard software and configurations as set by the UPPFI I.T. Officer.

15

Electronic Documents, Signatures, and Evidence

15.1. Recognition of Electronic Documents

Subject to policies to be promulgated by the UPPFI, 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.[1]

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:

1. the determination of the completeness of the document.
2. 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.

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

Legal Recognition of Electronic Documents

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 -

1. 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
2. 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)

15.2. Recognition of Electronic Signatures

Electronic signatures on an electronic document should be 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. Digital signatures (which are asymmetrically encrypted electronic signatures) from the Philippine National Public Key Infrastructure (PNPKI) shall not be discriminated against.[2]

15.3. 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.[3]

[2] To apply for Electronic Signature, see Guidelines on online application for digital signature, DPO Advisory Reference No. EBM 20-002 dated 11 May 2020.

[3] Sec. 2, Rule I, Rules on Electronic Evidence, A.M. No. 01-7-01-SC, July 17, 2001