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:

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.

3.2. Online Access to Personal Data

3.3. Remote Access

3.4. Remote Disconnection and Wiping

3.5. Guest Access, Separate Guest Network, Third-Party Connection

3.6. Virtual Private Network (VPN)

4

Communications and Email Policy

5

Website and Cookie Policy

6

Acceptable User Policy

7

Password/ Passphrase Policy

8

Backup Policy

8.1. What to Backup

8.2. How to Backup

8.3. Data Recovery Capability

9

Technical Incident Response and Reporting Policy

10

Personal Data Breach Management

10.1. Securing Incident Management Policy

10.2. Threats, Risks, and Vulnerabilities

10.3. Data Breach Response Team

11

Wireless Policy and Network Security Policy

11.1. Network Security Policy

11.2. Wireless Policy

12

Encryption Policy

12.1. Encryption Standard

12.2. Encryption of Computing Assets

12.3. Encription of Personal Information

13

Device Policies

13.1. Storage Device Policy

13.2. Mobile Device Policy

13.3. Cloud Policy

14

Security Policies

14.1. Inventory of Authorized and Unauthorized Devices

14.2. Standard Configurations for Different Computers

15

Electronic Documents, Signatures, and Evidence