

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

REVISION HISTORY			
Rev No	Description of change	Author	Effective Date
1	New Procedure	Chief Operations Officer (COO)	14 Oct 2015
2	No Change	Chief Operations Officer (COO)	12 Oct 2016
3	No Change	Chief Operations Officer (COO)	11 Oct 2017
4	No Change	Chief Operations Officer (COO)	10 Oct 2018
5	No Change	Chief Operations Officer (COO)	09 Oct 2019
6	No Change	Chief Operations Officer (COO)	18 Oct 2020
7	No Change	Chief Operations Officer (COO)	06 Sep 2021



UNIVERSITY OF PASADENA (UPAS)
Operational Procedures

Doc #: PO-OP-12.1	Title: Data Management System	
Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

1. Purpose

11 The Data management policy provides a framework to safeguard and protect the university’s data while providing flexibility to support the broad range of academic, research and administrative activities. UPAS maintains a zero tolerance for confidentiality and security violations, either intentionally or recklessly. The Institution requires that all files are shared online, and no physical copy is made unless it is specifically requested by the student.

12 This policy also defines the data management system to record and archive salient information in an accurate and timely manner so that UPAS can use this information to carry out evaluations and to support decision making at all levels of the organization.

2. Scope

21 This procedure applies to data and information related to students, faculty, staff, finance and Human resource and to all UPAS employees who have access to this information.

3. Definitions

31 Data -means information in a form which can be processed and is a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information.

4. Responsibility

41 The Chief Operation Officer (COO) is responsible for the effective implementation of the policy.

5. Procedure/Process:

51 Data Owner: Every set of data must have a Data Owner. The Data Owner has overall responsibility for the quality and integrity of the data. Specifically, the Data Owner is responsible for:

- Deciding the criticality and sensitivity of the data and classifying the data accordingly

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

- Authorizing access to Data
- Authorizing the use of the data, e.g. what processing takes place on the data
- Regularly reviewing access privileges
- Assessing the risks to the data include but are not limited to theft, data loss – due to lack of proper backups, neglect old hardware being recycled without proper data sanitization and Online File Share
- Data Users and Data Custodians need to be made aware of the potential consequences of data theft or loss so the relevant parties can act so as to mitigate these risks;
- Ensure that appropriate contingency plans are in place to safeguard the data and ensure that they or the Data Custodian have the appropriate backup and disaster recovery plans in place.
- The Data Owner is the most senior person in the area within which the data is created unless this role has been explicitly delegated to someone else.
- In the case of the data for the central systems in the University, relating examples are given in this table.

Functional Area	Academic Data	Administrative Data	Financial Data
Data owner	Chief Academic officer	Chief Operating Officer	Chief Financial Officer

5.2 The Data Custodian:

- In many cases data will be entrusted to an individual or a department, administrative unit/research unit (e.g. IT Services) for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian.
- This relationship between owner and custodian is often managed by a contract or service level agreement which clarifies specific responsibilities for each party,

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

typical Data Custodian responsibilities include:

- Maintaining the integrity and confidentiality of the data entrusted to them;
- Ensuring that access to the data is restricted to those individuals authorized by the data owner;
- Ensuring that processes undertaken on the data have been authorized by the data owner;
- Having adequate backup and recovery procedures in place for the data, taking into account the sensitivity and criticality of the data as characterized by the Data Owner;
- Providing any information necessary for the Data Owner to fulfil their responsibilities.

5.3 The Data Users

- Anyone using or processing University Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data always.
- They must comply with the relevant policies of the University (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright. The data should only be used for the purposes approved by the data owner
- Data Users are responsible for protecting their access privileges – Usernames and Passwords for University Systems should not be shared.
- Users should be especially vigilant in complying with this policy when transferring data to mobile equipment such as laptops, tablet devices, phones, USB memory sticks, PDAs, DVDs etc., as they have a greater risk of being lost or stolen.
- Anyone accessing information systems remotely to support the business activities of the University must be authorized to do so by the Data Owner of this data.

5.4 Security of data

- The university monitors and maintains electronic records through delegated password-protected access.
- All employees are required to have strong passwords and their passwords need to be changed every 60 days.

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

- The institution maintains all its in cloud, which is secured by a strong password. These records are accessible only by the staffs that have a need to know
- The cloud service provider does a backup of the records with a clear revision history of who accessed the files.
- [G-Suite platform - Data Access and restrictions](#)
- [G-Suite platform - Data Security and Compliance](#)
- [G-Suite platform – Data processing](#)
- [G-Suite Privacy Notice](#)

55 Data Integrity, validation and correction

- Data accuracy
 - recorded *accurately*
 - cross-checked for errors
 - not intentionally misleading (prevents fraudulent entries, editable entries)
- Data integrity/validation
 - genuine, true data
 - validated and supported/witnessed; vs intentionally falsified
 - relevant to the reporting requirement
 - not changeable after original record-keeping entry (extensively tracked changes)
- Legibility
 - clarity
 - legible (readable by anyone, removing guesswork)
 - readily accessible
- To ensure data integrity, once the data is stored electronically, it comes under version-controlled system which can track the changes along with the identify, date and time (provided by Google drive and report taken by G Suite reports).
- Each Data Owner, in conjunction with the appropriate Data Custodian, shall be responsible for developing a plan for their functional area to assess the risk of erroneous or inconsistent data and indicate how such Data, if found, will be corrected. The Quality and compliance Officer will be responsible for ensuring that each functional area uses that plan to develop and implement processes for identifying and correcting erroneous or inconsistent data.

	UNIVERSITY OF PASADENA (UPAS) Operational Procedures		
	Doc #: PO-OP-12.1	Title: Data Management System	
	Rev #: 07	Approved By: Chief Executive Officer (CEO)	Date: 06 Sep 2021

5.6 Backup data

- The University requires that all files are shared online, and physical copy is made only for student records.
- Only when required, hard copy of the data is made and are stored in locked filing cabinets.
- All archived student files are kept as quality records and shall be retained by the university.
- All data is maintained electronically in G-Suite platform which provides data backup as part of google drive services.

5.7 Any requests to deviate from or modify this policy or these retention periods must be made to and approved by the compliance officer

6. Review

The University of Pasadena reviews data management system policy every year.