| | UNIVERSITY OF PASADENA (UPAS)<br>Operational Procedures | | |
|---|---|---|---|
| | Doc # :PO-OP-12.1 | Title: Data Management System | |
| | Rev # : 05 | Approved By: Chief Executive Officer (CEO) | Date : 09 Oct 2019 |

| 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 |

1. **Purpose**

1.1 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.

1.2 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**

2.1 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**

3.1 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**

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

5. **Procedure/Process**

5.1 Data Controller: It is the data controller's responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability.

5.2 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

- 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 | Student Data | Administrative data | Financial data |
|---|---|---|---|
| Data Owner | Chief Academic Officer | Chief Operation Officer | Chief Financial Officer |

5.3 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, 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.

5.4 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 at all times.
- 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.

5.5 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.

- 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 - https://gsuite.google.com/learn-more/security/security-whitepaper/page-7.html
- G-Suite platform - Data Security and Compliance - https://static.googleusercontent.com/media/gsuite.google.com/en//intl/en/files/google-apps-security-and-compliance-whitepaper.pdf
- G-Suite platform - Data processing https://gsuite.google.com/terms/dpa_terms.html
- G-Suite Privacy Notice - https://gsuite.google.com/terms/education_privacy.html

5.6 Data Integrity, validation and correction

- University ensure Good Documentation Practices
    - **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

- The Institution ensures that the Data owner (or representative) reviews all images and electronic documents before they are accepted into the system to ensure data accuracy and legibility.
- 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).
- All University Data must be safeguarded and managed in all formats and media (e.g., print and digital), across all University systems through coordinated efforts and shared responsibilities. 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 Chief 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.

5.7 Backup data

- The University requires that all files are shared online and physical copy is made only for student records.
- 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 option as part of google drive service.
- Additional backup of these records is done daily and copied to a RAID System with dual HDD backup.

## 6. Review

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