

**Institute of Primate Research**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOP No.** | **Issue Number** | **Issue Date** | **Revision Status** | **Revision Date** |
| **SOP/KIPRE/RPD/DSAS/3.1.76** | **Version 01** | **October 2025** | **-** | **-** |

**STANDARD OPERATING PROCEDURE (SOP) DOCUMENT**

**Data storage, backup, encryption, and disaster recovery**

|  |  |  |  |
| --- | --- | --- | --- |
| **Approvals** |  |  |  |
|  | **Name** | **Signature** | **Date** |
| **Developed by:** | \_Patrick Waweru Mwaura\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_6th October; 2025\_** |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Reviewed by:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Approved by:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[1. PURPOSE 4](#_Toc144316958)

[2. SCOPE 4](#_Toc144316959)

[3. PERSONS RESPONSIBLE: 4](#_Toc144316960)

[4. FREQUENCY 4](#_Toc144316961)

[5. MATERIALS 4](#_Toc144316962)

[6. PROCEDURE 4](#_Toc144316963)

[7. REFERENCES 5](#_Toc144316964)

# 

# PURPOSE

To define secure storage, backup, encryption, and recovery procedures ensuring availability, integrity, and confidentiality of all DS&AS datasets.

# SCOPE

Applies to all data (raw, processed, and metadata) managed by DS&AS, including on premise servers and cloud platforms.

# PERSONS RESPONSIBLE:

* **Data Engineer:** Implements storage, backup, and encryption.
* **ICT Lead:** Ensures infrastructure resilience.
* **Head of DS&AS:** Monitors compliance with policy.

# FREQUENCY

* Backups conducted **daily** (incremental) and **weekly** (full).
* Disaster recovery drills conducted **annually**.

# MATERIALS

* Secure servers/cloud (PostgreSQL, MySQL, AWS/Azure).
* Encryption tools (AES-256, SSL/TLS).
* Backup automation software.
* Disaster Recovery (DR) plan.

# PROCEDURE

1. **Storage:** Store datasets in centralized repository with role-based access.
2. **Encryption:** Encrypt all sensitive datasets at rest and in transit.
3. **Backups:** Automate daily incremental and weekly full backups; test restore monthly.
4. **Disaster Recovery:** Maintain offsite/cloud backup; initiate DR plan in case of system failure.
5. **Monitoring:** DS&AS reviews storage/backup logs weekly.

# REFERENCES

To be provided later