Institute of Primate Research

STANDARD OPERATING PROCEDURE (SOP) DOCUMENT

Data storage, backup, encryption, and disaster recovery

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

Approvals

	Name	**Signature**	**Date**
Developed by:	_Patrick Waweru Mwaura_	_____	**_6th October; 2025_**
	_____	_____	_____
	_____	_____	_____
Reviewed by:	_____	_____	_____
Approved by:	_____	_____	_____

Table of Contents

1. PURPOSE

To establish **standardized procedures for the secure storage, backup, encryption, and disaster recovery** of all DS&AS-managed datasets, ensuring their **availability, integrity, and confidentiality**.

This SOP ensures that:

- Raw and processed data are **securely stored and recoverable** in line with approved **study designs (SOP 3)** and **Statistical Analysis Plans (SOP 4)**.
- Outputs, reports, and dashboards are preserved to support **reproducibility and dissemination (SOP 5)**.
- All storage and recovery practices comply with **institutional policies (SOP 1)**, ethical and regulatory standards (SOP 2), and **data access controls (SOP 6)**.

By defining these procedures, DS&AS ensures continuity of research operations, regulatory compliance, and protection of sensitive biomedical, ecological, and primatological data.

2. SCOPE

Applies to all **raw, processed, and metadata** managed by DS&AS across **on premise servers, institutional repositories, and approved cloud platforms**.

It covers **data storage, encryption, backup scheduling, access restoration, and disaster recovery procedures** for all DS&AS-supported research projects.

3. PERSONS RESPONSIBLE:

- **Data Engineer:** Implements and maintains secure data storage, backup, encryption, and recovery systems.
- **ICT Lead:** Ensures infrastructure reliability, conducts system health checks, and coordinates disaster recovery testing.
- **Head of DS&AS:** Oversees policy compliance, approves data recovery actions, and reports on storage and backup integrity to institutional management.
- **Data Protection Officer (DPO):** Verifies adherence to data protection and privacy standards during storage and recovery processes**.**

4. FREQUENCY

- Incremental backups performed **daily** and full backups conducted **weekly**.
- Backup integrity verified **monthly** through checksum validation.
- Disaster recovery simulations conducted **annually** or after any major infrastructure change.
- Storage capacity and encryption compliance reviewed **quarterly**.

5. MATERIALS

- Secure data storage infrastructure (on-premise servers or approved cloud platforms such as **AWS**, **Azure**, or **Google Cloud**).
- Database management systems including **PostgreSQL**, **MySQL**, **Neo4j** (for graph data), and **text-based or document-oriented databases** (e.g., JSON, CSV repositories, MongoDB).
- Encryption tools and protocols (**AES-256**, **SSL/TLS**, and institutional key management systems).
- Automated backup and synchronization software.
- Documented **Disaster Recovery (DR) Plan** and **Business Continuity Policy**.
- Institutional **Data Retention and Archiving Policy** for long-term data stewardship.

6. PROCEDURE

- **Data Storage:**

  • All datasets (raw, processed, and metadata) are stored in the **centralized DS&AS data repository** with clearly defined access levels based on project roles.

  • Data must not be stored on personal devices or unsecured drives.

- **Encryption:**

  • All sensitive or confidential datasets are encrypted **at rest** using AES-256 and **in transit** using SSL/TLS or institutional VPN.

  • Encryption keys are managed through institutional key management systems under ICT oversight.

- **Backup Procedures:**
  - Automated **daily incremental** and **weekly full backups** are performed for all repositories.
  - Backup integrity is tested monthly by restoring random samples to verify data completeness and usability.
- **Disaster Recovery (DR):**
  - An **offsite or cloud-based backup** is maintained for all critical systems.
  - The **Disaster Recovery Plan** (DRP) is activated in case of major data loss, corruption, or infrastructure failure.
  - ICT and DS&AS jointly document all recovery steps and post-incident reviews.
- **Monitoring and Reporting:**
  - Backup and storage logs are reviewed weekly by DS&AS.
  - Quarterly summaries of storage performance, backup success rates, and DR drills are reported to the Head of DS&AS.

7. REFERENCES

1. Kenya Data Protection Act (2019) and Regulations.
2. KIPRE Institutional Data Protection and Sharing Policy (2024).
3. DS&AS SOP 6 – Data Access and Authentication Procedures.
4. DS&AS SOP 2 – Alignment with Institutional and National Regulations.
5. ISO/IEC 27001:2022 – Information Security Management Systems.
6. FAIR Data Principles (Wilkinson et al., 2016).
7. World Health Organization (WHO) Data Security and Privacy Guidelines.
8. National Commission for Science, Technology and Innovation (NACOSTI) Research Data Management Framework.
9. Federal Information Security Management Act (FISMA, 2002; amended 2014).
10. General Data Protection Regulation (GDPR) (EU) 2016/679.

8. APPENDIX

Appendix 7.1 – Forms and Templates

1. Data Storage and Encryption Checklist
2. Backup Verification Log Template
3. Disaster Recovery (DR) Test Report Template
4. Data Restoration Request Form
5. Access and Encryption Key Request Form
6. Backup and Storage Audit Report Template

Appendix 7.2 – Reference Systems

- Data Repositories: PostgreSQL, MySQL, Neo4j (graph database), and text-based repositories (CSV, JSON, XML).
- Cloud Platforms: AWS S3, Microsoft Azure, or institutional equivalents.
- Backup Tools: Rsync, Duplicati, or other approved automation tools.
- Encryption Tools: OpenSSL, GPG, or integrated database encryption modules.