Institute of Primate Research

STANDARD OPERATING PROCEDURE (SOP) DOCUMENT

Data Access and authentication procedures

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, **secure, and role-based data access and authentication procedures** for all DS&AS-managed datasets, ensuring that sensitive biomedical, ecological, and primatological data are **protected from unauthorized access or misuse**.

This SOP ensures that:

- Access aligns with ethical, regulatory, and institutional requirements, including the Kenya Data Protection Act (2019).
- All data access requests, approvals, and revocations are documented, auditable, and traceable.
- Data use is restricted to approved study designs and Statistical Analysis Plans (SAPs) to preserve reproducibility and compliance.
- Users are aware of their responsibilities regarding data privacy, confidentiality, and appropriate use.

This SOP builds upon:

- **SOP 1 – Policies and Strategies:** Governance, FAIR principles, and compliance frameworks.
- **SOP 2 – Alignment with Regulations:** Ethical approvals, regulatory compliance, and institutional policies.
- **SOP 3 – Study Design and Statistical Consultation:** Access linked to approved study designs and statistical requirements.
- **SOP 4 – Statistical Analysis Plans (SAPs):** Ensuring data is used according to pre-approved analyses.
- **SOP 5 – Reporting Research Results:** Access needed to generate reproducible and compliant outputs.

2. SCOPE

Applies to all users—internal and external—who require authorized access to DS&AS-managed databases, repositories, or analytic platforms.

It includes:

- Access to datasets across all research projects supported by DS&AS.
- Users with temporary or permanent roles requiring data interaction for approved research, analysis, or oversight activities.
- Management of user permissions and roles within institutional systems to ensure controlled and traceable access.

3. PERSONS RESPONSIBLE:

- **Head of DS&AS:** Oversees data access governance, approves access requests, and ensures adherence to institutional policies.
- **Data Engineer / ICT Officer:** Implements and maintains authentication controls, role-based permissions, and technical security measures.
- **Data Protection Officer (DPO):** Monitors compliance with the Kenya Data Protection Act (2019), reviews access audits, and advises on regulatory obligations.
- **Principal Investigator (PI) / Project Lead:** Requests access for project team members and validates the necessity of access for research purposes.

4. FREQUENCY

- **Quarterly Reviews:** All user access rights are reviewed every three months to ensure appropriateness and compliance.
- **Triggered Reviews:** Immediate review and adjustment of access upon staff role changes, project completion, or early termination of collaborations.
- **Audits:** Annual audit of all access logs to verify compliance with institutional policies and regulatory requirements.

5. MATERIALS

- **Institutional Access Control Policy:** Provides guidance on roles, permissions, and access levels.
- **Authentication Software:** Multi-factor authentication (MFA), VPN, LDAP/Active Directory, or equivalent systems to secure user login.
- **Data Classification Register:** Lists all datasets with sensitivity levels (e.g., PII, PHI, confidential, public).

- **Access Request Forms:** Standardized templates for requesting, approving, or modifying data access.
- **Audit and Monitoring Tools:** Logging systems and dashboards for tracking access events and generating compliance reports.
- **Version-Controlled Repository:** Central repository for storing approved access logs and associated documentation.

6. PROCEDURE

1. **Step 1: Request Submission**

   • User submits a completed **Data Access Request Form**, specifying datasets, purpose, duration, and required access level.

   • Request must be approved by the **Principal Investigator (PI) or Project Lead**.

2. **Step 2: Access Review and Approval**

   • DS&AS Head or delegated officer reviews the request, ensuring alignment with project requirements and compliance with data classification (Open, Restricted, Confidential).

   • Approved requests are forwarded to the **Data Engineer/ICT Officer** for implementation.

3. **Step 3: Authentication and Account Setup**

   • ICT enables user access using **role-based permissions**, multi-factor authentication (MFA), and VPN or secure network access.

   • Temporary or time-limited accounts are configured where applicable.

4. **Step 4: Logging and Monitoring**

   • All data access events are automatically logged, including **user ID, dataset accessed, date/time, and action performed**.

   • DS&AS and DPO periodically review logs to detect unauthorized access or suspicious activity.

5. **Step 5: Access Maintenance and Review**

   • **Quarterly reviews** of all active accounts are conducted to ensure appropriateness.

   • Access is **revoked immediately** upon project completion, staff role changes, or policy violations.

6. **Step 6: Audit and Compliance Reporting**

   • Annual audits are conducted by DS&AS and the DPO to verify compliance with institutional policies and the Kenya Data Protection Act (2019).

   • Findings are documented and corrective actions implemented if discrepancies are identified.

7. REFERENCES

1. **Kenya Data Protection Act (DPA) 2019** – Legal framework for protection of personal data and regulation of processing activities.
2. **KIPRE Institutional Data Protection and Sharing Policy (2024)** – Institutional guidance on data governance and access control.
3. **FAIR Data Principles** – Standards for Findable, Accessible, Interoperable, and Reusable data.
4. **SOP 1 – Policies and Strategies** – Governance frameworks for DS&AS operations.
5. **SOP 2 – Alignment with Regulations** – Ethical and regulatory compliance guidance.
6. **SOP 3 – Study Design and Statistical Consultation** – Ensures access aligns with approved study designs.
7. **SOP 4 – Statistical Analysis Plans (SAPs)** – Ensures access is restricted to approved analyses.
8. **SOP 5 – Reporting Research Results** – Access required for generating reproducible reports and dashboards.
9. **ISO/IEC 27001:2013** – International standard for information security management.

8. **APPENDICES**

1. **Appendix A: Data Access Request Form**
   - User details (name, role, institution)
   - Project/study ID
   - Dataset(s) requested
   - Purpose of access
   - Requested duration and access level (Open, Restricted, Confidential)
   - PI/Project Lead approval signature
   - Head of DS&AS approval signature

2. **Appendix B: Access Review Checklist**
   - Compliance with ethical approvals and DPA 2019
   - Alignment with approved study design and SAP
   - Verification of role-based access necessity
   - Expiration and revocation date verification

3. **Appendix C: User Roles and Permissions Table**

Role	Access Level	Dataset Type	Notes
Analyst	Read/Write	Restricted	Requires PI approval
PI	Read/Write	Confidential	Full project datasets
Collaborator	Read-only	Open/Restricted	Limited to assigned datasets
Auditor	Read-only	All	For compliance review only

4. **Appendix D: Access Log Template**

   1. User ID

   2. Dataset accessed

   3. Date/Time of access

   4. Action performed (View, Download, Modify)

   5. Authorized by

   6. Notes / Observations