Standard Operating Procedure (SOP)

Data Collection Source Verification and Authorization

Purpose: This SOP defines the procedures for **data collection source verification and authorization**, including the identification and validation of data sources, verification of data accuracy and reliability, authorization protocols for data access and collection, documentation of source credentials, and compliance with data privacy and security standards. The objective is to ensure the integrity and authenticity of collected data by implementing robust verification and approval processes.

1. Scope

This SOP applies to all personnel and processes involved in the collection, verification, and authorization of data sources within the organization.

2. Roles and Responsibilities

Role	Responsibility
Data Collector	Identify, record, and initiate verification of data sources.
Data Verifier	Validate and approve the accuracy and reliability of data sources.
Data Owner	Authorize access to data sources and ensure compliance with all applicable standards.
Data Protection Officer	Ensure compliance with data privacy and security regulations.

3. Procedures

1. **Source Identification**
   - List all potential data sources relevant to the data collection project.
   - Maintain an inventory of data sources, including source type, ownership, and access details.
2. **Source Validation**
   - Assess credibility of sources based on reputation, recency, and relevance.
   - Confirm source documentation and credentials (e.g., source certificates, official records).
3. **Data Accuracy and Reliability Verification**
   - Cross-check data from multiple independent sources where possible.
   - Record any discrepancies and document resolution steps.
4. **Authorization Protocols**
   - Review and approve data collection requests by designated Data Owners.
   - Grant and record access permissions according to organizational policy.
   - Maintain an audit trail of all access and authorization actions.
5. **Documentation of Source Credentials**
   - Document source credentials, including issuer, validity period, and verification date.
   - Archive supporting documents in the secure data repository.
6. **Compliance with Data Privacy and Security**
   - Adhere to applicable data privacy laws and security standards (e.g., GDPR, HIPAA).
   - Implement encryption and access controls for sensitive data.
   - Ensure all collection and storage mechanisms meet organizational policy.

4. Documentation

- Source Inventory Log
- Source Validation Checklist
- Authorization Records
- Audit Trail
- Data Privacy Compliance Reports

5. Review and Update

This SOP must be reviewed annually or when significant changes in data collection processes or applicable regulations occur. All updates must be documented and communicated to relevant personnel.

6. References

- Organizational Data Management Policy
- Applicable Data Privacy Regulations (e.g., GDPR, HIPAA)
- Data Security Standards

7. Approval

Name	Title	Signature	Date