Standard Operating Procedure (SOP): Archival and Secure Deletion of Obsolete Data

This SOP details the procedures for **archival and secure deletion of obsolete data**, including identification of data eligible for archiving or deletion, secure data transfer to archival storage, implementation of encryption and access controls, verification of data integrity post-transfer, schedules and policies for data retention, methods for secure deletion to prevent data recovery, compliance with legal and regulatory requirements, and documentation of all archival and deletion activities to ensure data privacy and organizational security.

1. Purpose

To define the standards, guidelines, and procedures for the archival and secure deletion of obsolete data to uphold data privacy, maintain compliance, and protect organizational information assets.

2. Scope

This SOP applies to all electronic and physical data owned, managed, or processed by the organization and covers all departments, staff, and third-party service providers involved in data management.

3. Definitions

- **Obsolete Data:** Data that is no longer actively used or required for operational, legal, or regulatory purposes.
- **Archival Storage:** Storage designated for long-term preservation of infrequently accessed data.
- **Secure Deletion:** Methods applied to permanently and irrecoverably erase data.

4. Responsibilities

- **Data Owners:** Identify obsolete data and authorize archiving or deletion.
- **IT/Data Management Teams:** Execute archival and deletion in accordance with this SOP.
- **Compliance Officer:** Ensure all activities comply with legal and regulatory requirements.

5. Procedure

1. **Identification of Obsolete Data**
    - Review data inventories to locate data no longer needed.
    - Evaluate against retention schedules and legal requirements.

2. **Data Archival**
    - Transfer eligible data to designated archival storage using secure channels (e.g., encrypted network transfer).
    - Apply encryption and strict access controls to archived data.
    - Log and document all data transfers.

3. **Verification of Data Integrity**
    - Verify checksums or hashes post-transfer to confirm data integrity.

4. **Retention Schedule**
    - Store archived data for the period specified in organizational, legal, or regulatory policies.

5. **Secure Deletion of Data**
    - Ensure data marked for deletion is destroyed using approved secure deletion tools (e.g., cryptographic erasure, multi-pass overwriting, degaussing for physical media).
    - Document each deletion request and completion.

6. **Compliance and Legal Review**
    - Verify all archival and deletion complies with GDPR, HIPAA, or other relevant regulations.
    - Consult legal where data is subject to litigation hold or special regulations.

7. **Documentation and Reporting**

- Maintain an audit log of all data archival and deletion operations.
- Perform periodic audits and report findings to management.

6. Records Management

- Retain all documentation and logs related to data archival and deletion for a minimum of [X] years, or as required by law.

7. Compliance

- All procedures must comply with applicable laws and industry regulations.
- Refer to the organization's Data Privacy Policy and Information Security Policy for additional guidance.

8. Review and Revision

- This SOP will be reviewed annually or as needed to accommodate changes in regulations, technology, or organizational policies.

Non-compliance with this SOP may result in disciplinary actions and could expose the organization to legal risks.

Effective Date: [YYYY-MM-DD]

Document Owner: [Name/Department]

Revision History: [Version, Date, Description of Changes]