Standard Operating Procedure (SOP): Secure Disposal of Sensitive Data from Storage Media

1. Purpose:
The purpose of this SOP is to establish a standardized process for securely disposing of sensitive data stored on various storage media to prevent unauthorized access and ensure compliance with data privacy regulations.

2. Scope:
This SOP applies to all personnel involved in managing and disposing of storage media containing sensitive data within the organization.

3. Responsibilities:
- Data Owners: Responsible for identifying and classifying sensitive data that requires secure disposal.
- IT Department: Responsible for overseeing the secure disposal process and providing the necessary tools and resources.
- IT Support Team: Assists in identifying storage media containing sensitive data and coordinating their disposal.
- Data Protection Officer (if applicable): Ensures compliance with data protection regulations and provides guidance on secure data disposal.

4. Prerequisites:
- Understanding of the organization's data classification policies and procedures.
- Knowledge of secure data disposal methods and tools.

5. Procedures:

5.1. Identify Sensitive Data and Storage Media:
  - Collaborate with data owners and department heads to identify storage media that contain sensitive data to be disposed of securely.
  - Classify the sensitivity level of the data based on the organization's data classification policy.

5.2. Determine Disposal Method:
  - Determine the appropriate disposal method based on the type of storage media and the sensitivity of the data. Options may include physical destruction, degaussing, or secure data wiping.

5.3. Physical Destruction:
  - For storage media such as hard drives, USB drives, or optical discs:
    - Use an industrial shredder or disintegration equipment to physically destroy the media.
    - Ensure the destruction process renders the media unreadable and irrecoverable.

5.4. Degaussing:
  - For magnetic storage media such as hard drives or magnetic tapes:
    - Use a degausser to demagnetize the media, rendering the data unreadable.
    - Follow the manufacturer's guidelines for proper degaussing procedures.

5.5. Secure Data Wiping:
  - For reusable storage media such as hard drives or solid-state drives:

- Use data wiping software that conforms to recognized standards (e.g., NIST SP 800-88) to overwrite the entire storage media with random data or zeros.
- Perform multiple passes to ensure data eradication.

5.6. Documentation:

- Maintain records of all storage media disposed of, including the type of media, disposal method used, date of disposal, and responsible personnel.
- Document any exceptions or incidents encountered during the disposal process.

6. References:

- Organization's data classification policy.
- Data protection regulations (e.g., GDPR, HIPAA).

7. Definitions:

- Sensitive Data: Information that, if accessed or disclosed, could result in harm to individuals, the organization, or violate legal or regulatory requirements.

8. Revision History:

- Version 1.0: [17MAY2023] - [David Siebert]
  - Initial draft of the SOP.
- Version 1.1: [Date] - [Contributor Name]
  - Incorporated feedback from stakeholders.
  - Added secure data wiping procedure.
- Version 1.2: [Date] - [Contributor Name]
  - Reviewed and refined the SOP for clarity and completeness.