Standard Operating Procedure (SOP)

Document Classification and Labeling Procedures

This SOP describes **document classification and labeling procedures** to ensure consistent identification, organization, and management of documents. It covers criteria for document categorization, labeling standards, handling of confidential and sensitive information, and guidelines for proper storage and retrieval. The purpose is to enhance document security, accessibility, and compliance with regulatory requirements through systematic classification and clear labeling practices.

1. Purpose

To establish systematic procedures for classifying and labeling documents to ensure security, accessibility, and regulatory compliance.

2. Scope

This SOP applies to all organizational documents, both in physical and electronic form, across all departments and employees handling such documents.

3. Responsibilities

- All employees must correctly classify and label documents according to this SOP.
- Department heads are responsible for monitoring compliance.
- The Document Control Officer oversees implementation and periodic review.

4. Classification Criteria

All documents must be reviewed and classified into one of the following categories:

Classification Level	Description	Example
Confidential	Highly sensitive information; access strictly limited.	Personnel records, financial reports, legal documents.
Restricted	Internal information requiring limited access and oversight.	Project plans, vendor agreements.
Internal Use Only	Non-public information accessible only to staff.	Internal memos, process manuals.
Public	Information approved for open, public dissemination.	Press releases, published reports.

5. Labeling Standards

Each classified document must be clearly labeled with its appropriate classification. Labels should appear on the header or footer (for electronic documents) or on the cover/page header (for physical documents).

- **CONFIDENTIAL**
- **RESTRICTED**
- **INTERNAL USE ONLY**
- **PUBLIC**

Labels must be:

- In uppercase letters
- Easily visible in all document versions
- Applied to both electronic and printed copies

6. Handling Confidential and Sensitive Information

- Limit access to individuals with a validated need-to-know.
- Transmit only via secured methods (e.g., encrypted email, locked filing).
- Do not leave sensitive documents unattended or unsecured.
- Report any suspected data breaches immediately to the Document Control Officer.

7. Storage and Retrieval Guidelines

- Store physical documents in secure, access-controlled locations.
- Maintain electronic documents on secure, access-restricted servers or repositories.
- Ensure accurate indexing for quick and secure document retrieval.
- Regularly back up electronic documents and test recovery processes.

8. Review and Disposal

- Review classifications periodically and update labels as needed.
- Dispose of documents securely:
  - Use shredding for physical confidential documents.
  - Permanently delete electronic files (with no recoverability) for sensitive records.

9. Compliance and References

- This SOP must be aligned with applicable regulatory and industry requirements (e.g., GDPR, HIPAA, ISO 27001).
- Refer to the Organization's Document Management Policy for additional details.

10. Revision History

Version	Date	Description of Change	Approved By
1.0	2024-06-01	Initial release	Document Control Officer