SOP: Classification and Labeling of Confidential Information

This SOP defines the **classification and labeling of confidential information**, detailing procedures for identifying, categorizing, and marking sensitive data to ensure its protection. It covers the criteria for different confidentiality levels, proper labeling techniques, handling protocols, access control measures, and compliance with data privacy regulations. The objective is to safeguard confidential information from unauthorized access, disclosure, and misuse throughout its lifecycle.

1. Scope

This SOP applies to all employees, contractors, and third-party partners involved in handling organizational data in any format (physical or electronic).

2. Definitions

- **Confidential Information:** Any data that, if disclosed without authorization, could harm the organization or individuals.
- **Labeling:** The process of marking information according to its confidentiality classification.
- **Data Owner:** The individual responsible for determining the classification level of specific information.

3. Classification Levels

Level	Description	Examples	Label
Confidential	Strictly limited to authorized individuals; unauthorized disclosure could cause significant harm.	Financial records, trade secrets, PII, passwords	CONFIDENTIAL
Restricted	Limited distribution within the organization; unauthorized disclosure could cause moderate harm.	Project documents, non-public business plans	RESTRICTED
Internal	Accessible to all employees; unauthorized disclosure has minimal impact.	Internal memos, process manuals	INTERNAL
Public	Approved for release to the public; no adverse impact if disclosed.	Press releases, published reports	PUBLIC

4. Responsibilities

- **Data Owners:** Determine and assign appropriate classification.
- **Employees:** Adhere to classification, labeling, and handling protocols; report any incidents of unauthorized disclosure.
- **IT & Security Teams:** Support enforcement of access controls and monitor compliance.

5. Labeling Procedures

1. Review information for sensitivity and potential impact of disclosure.
2. Assign the appropriate classification level as outlined above.
3. Mark physical documents with the classification label in the header/footer of each page.
4. Apply electronic labels in file properties, document headers, or filenames (e.g., `Confidential_[DocumentName].pdf`).
5. For email, include classification in the subject line and email footer.

6. Handling and Access Control

- Access to classified information is restricted based on classification level and role-based access controls.
- Store confidential information in secured locations or encrypted formats.
- Do not share classified information via unsecured channels.
- Dispose of confidential materials securely (e.g., shredding, secure deletion).

7. Compliance and Review

- All employees must comply with applicable data privacy laws/regulations (e.g., GDPR, HIPAA).
- This SOP shall be reviewed annually and updated as necessary.

8. Incident Reporting

- Report any suspected or actual unauthorized disclosure of confidential information immediately to the Information Security team.
- Follow organizational incident response procedures.