SOP: Confidentiality and Security of Controlled Documents

This SOP establishes the protocols for maintaining the **confidentiality and security of controlled documents**, including proper document classification, access control, storage, distribution, and disposal. It aims to protect sensitive information from unauthorized access, ensure document integrity, and support compliance with regulatory and organizational requirements.

SOP Number	[Assign SOP Number]	**Effective Date**	[Effective Date]
Version	[Version]	**Review Date**	[Review Date]
Approval	[Approver Name & Title]		

1. Purpose

To define the procedures for protecting the confidentiality and security of all controlled documents (electronic and hard copy) throughout their lifecycle.

2. Scope

This SOP applies to all employees and contractors who create, access, manage, or dispose of controlled documents within the organization.

3. Definitions

- **Controlled Document:** Any document identified as subject to regulated or business-critical handling and protection.
- **Confidential Information:** Data not intended for public disclosure due to legal, regulatory, or business reasons.
- **Access Control:** Methods used to ensure only authorized individuals can view, edit, or distribute documents.

4. Responsibilities

- **Document Owners:** Classify, authorize access, and ensure proper management of documents.
- **IT/Admin Teams:** Provide secure systems and monitor access.
- **All Staff:** Adhere to this SOP and report breaches or risks.

5. Procedures

1. **Document Classification**
    - Classify documents according to sensitivity: e.g., Confidential, Internal Use Only, Public.
    - Label documents clearly with classification level.
2. **Access Control**
    - Restrict access to authorized personnel only.
    - Regularly review and update access permissions.
    - Use password protection, encryption, or secure file systems for electronic documents.
3. **Document Storage**
    - Store hard copies in locked cabinets or secure rooms.
    - Use secure servers or approved cloud storage for electronic documents.
    - Ensure backup systems are in place and regularly tested.
4. **Distribution**
    - Distribute only to authorized personnel, using secure transmission methods (e.g., encrypted email, secure file transfer).
    - Log and track document distribution as needed.
5. **Document Disposal**
    - Shred physical documents or use secure disposal services.
    - Permanently delete electronic files and remove from backups as appropriate.
    - Document and, if required, witness disposal of highly sensitive information.
6. **Incident Reporting**

- Immediately report any loss, unauthorized access, or breach to management and IT.
- Follow incident response procedures.

6. Training

All relevant staff must complete training on document confidentiality and security procedures upon hiring and annually thereafter.

7. Compliance

Compliance with this SOP is mandatory. Non-compliance may result in disciplinary action in accordance with HR and legal policies.

8. References

- Applicable regulations (e.g., GDPR, HIPAA)
- Company Information Security Policy

9. Revision History

Version	Date	Description	Approved By
[Version]	[Date]	Initial Version	[Name]