SOP: Inspection Records Retention and Data Management Protocol

This SOP details the **inspection records retention and data management protocol**, encompassing the procedures for systematic documentation, secure storage, timely retrieval, and authorized disposal of inspection records. It ensures compliance with regulatory requirements, maintains data integrity and confidentiality, facilitates efficient audits, and supports continuous improvement through accurate record-keeping and data analysis.

1. Purpose

To establish standardized procedures for retaining, managing, and disposing of inspection records, ensuring regulatory compliance, data integrity, and information security.

2. Scope

This SOP applies to all staff involved in the creation, management, storage, and disposal of inspection records, regardless of format (paper or electronic).

3. Definitions

- **Inspection Records:** Documents generated as evidence of inspection activities, including forms, checklists, photos, reports, and correspondence.
- **Retention Period:** The period records must be kept to comply with legal, regulatory, or organizational requirements.
- **Secure Storage:** Physical or electronic means to prevent unauthorized access, alteration, or loss.
- **Authorized Disposal:** Secure destruction of records that have met retention requirements.

4. Responsibilities

- **Record Owners:** Ensure accurate, timely, and complete documentation of inspection activities.
- **Records Management Team:** Monitor, store, retrieve, and dispose of inspection records according to this SOP.
- **IT Department:** Ensure the security of electronic records and maintain backup systems.
- **Compliance Officer:** Verify adherence to applicable regulations and this SOP.

5. Procedure

5.1 Documentation

- Complete all inspection records promptly, accurately, and legibly.
- Label records with unique identifiers (e.g., inspection date, number, and location).
- Digitally scan paper records when possible and store in the approved document management system.

5.2 Secure Storage

- Store paper records in locked, access-controlled cabinets or rooms.
- Maintain electronic records in password-protected systems with restricted access based on user roles.
- Back up electronic records at regular intervals according to IT policy.
- Protect records against unauthorized access, damage, or loss.

5.3 Retention and Retrieval

- Refer to the records retention schedule (Section 6) to determine the minimum retention period.
- Ensure efficient retrieval of records for audits, inspections, or management reviews.

5.4 Disposal

- Identify records eligible for disposal according to the retention schedule.
- Obtain written approval from the Compliance Officer before destruction.
- Shred physical records and securely delete electronic files, ensuring data is irrecoverable.
- Document all disposals with date, method, and responsible person.

6. Records Retention Schedule

Record Type	Minimum Retention Period	Storage Location
Inspection Reports	5 years	Electronic DMS / Secure Archive
Checklists & Forms	3 years	Electronic DMS / Locked File Cabinet
Photos & Supporting Documents	5 years	Electronic DMS
Correspondence Related to Inspections	5 years	Electronic Mail System / DMS
Audit Trails & Access Logs	2 years	IT System Logs

**Note: Adjust retention periods as required by applicable regulations or organizational policy.*

7. Data Integrity and Confidentiality

- Audit all changes or deletions to electronic records with date, user, and action logged.
- Encrypt sensitive data both at rest and during transmission.
- Limit access to records based on role, with regular reviews of user permissions.
- Train all staff on confidentiality standards and data protection practices.

8. Continuous Improvement

- Periodically review this SOP and associated records for gaps or improvement opportunities.
- Incorporate feedback from audits and regulatory inspections.
- Update documentation and staff training as necessary.

9. References

- Applicable national, regional, and local regulatory requirements.
- Company Records Management Policy.
- IT Security Policy.

10. Revision History

Version	Date	Description	Approved By
1.0	2024-06-09	Initial release	[Name/Position]