Standard Operating Procedure (SOP)

Incident Report Filing, Record Retention, and Confidentiality Procedures

This SOP details the **incident report filing, record retention, and confidentiality procedures**, including the proper documentation of incidents, timely submission of reports, secure storage of records, compliance with legal and organizational retention requirements, and safeguarding sensitive information to protect privacy and maintain confidentiality. The goal is to ensure accurate, accessible, and secure management of incident records to support accountability and continuous improvement.

1. Purpose

- To establish standardized procedures for filing incident reports, retaining incident records, and maintaining confidentiality.
- To ensure legal and organizational compliance, data integrity, accountability, and privacy protection.

2. Scope

- This SOP applies to all employees, contractors, and stakeholders involved in reporting, documenting, storing, and accessing incident records within the organization.

3. Definitions

Term	Definition
Incident	An unplanned event that may result in injury, damage, security breach, or organizational disruption.
Incident Report	Official documentation detailing the nature, facts, and response to an incident.
Retention Period	The length of time records must be kept before destruction or archiving.
Confidentiality	The obligation to protect sensitive or personal information from unauthorized disclosure.

4. Procedures

4.1 Incident Report Filing

- Immediately document all pertinent details of the incident using the approved Incident Report Form.
- Include the date, time, location, individuals involved, description of the event, actions taken, and witnesses.
- Submit the completed incident report to the designated supervisor or department within **24 hours** of occurrence.
- Reports must be signed and dated by the reporting individual.

4.2 Report Review and Submission

- The supervisor or designated official must review and acknowledge receipt of the report within **48 hours**.
- Initiate any required investigations or follow-up actions.
- Forward the report to the Records & Compliance Office for storage.

4.3 Record Retention

- Incident records must be retained in accordance with legal and regulatory requirements (see Section 6 below).
- Maintain records in secure, access-controlled physical or electronic storage.
- At the conclusion of the retention period, records shall be securely destroyed or archived.

4.4 Confidentiality and Access Control

- Incident reports and related records are confidential and accessible only to authorized personnel.
- All staff must protect incident records from unauthorized access, use, disclosure, alteration, or destruction.
- Electronic records should be password-protected; physical records should be stored in locked cabinets.
- Unauthorized sharing or discussion of incident details is strictly prohibited and may result in disciplinary action.

5. Responsibilities

- **All Employees:** Report incidents promptly and accurately; maintain confidentiality.
- **Supervisors/Managers:** Ensure proper review, submission, and follow-up of incident reports.
- **Records & Compliance Office:** Oversee retention, storage, access control, and secure destruction of records.

6. Record Retention Table

Record Type	Minimum Retention Period	Disposal Method
Incident Reports	7 Years	Shredding (paper) / Permanent deletion (digital)
Investigation Records	7 Years	Shredding / Deletion
Related Correspondence	7 Years	Shredding / Deletion

Note: Longer retention may apply under certain legal, regulatory, or organizational policies.

7. Confidentiality and Security Measures

- All staff must sign confidentiality agreements and complete periodic data privacy training.
- Audits shall be conducted annually to ensure compliance with confidentiality and retention protocols.
- Any breach of confidentiality or unauthorized access must be reported immediately to the Compliance Officer.

8. References

- Relevant laws and regulations (e.g., GDPR, HIPAA, local data protection statutes)
- Organizational policies on privacy and records management