Standard Operating Procedure (SOP): Reporting and Documentation Requirements

1. Purpose

This SOP details the **reporting and documentation requirements** essential for maintaining accurate records of incidents, safety checks, compliance audits, and operational activities. It ensures timely and systematic reporting procedures, standardization of document formats, proper record-keeping, confidentiality protocols, and regular review to support accountability, legal compliance, and continuous improvement within the organization.

2. Scope

This procedure applies to all staff involved in reporting, record-keeping, or reviewing organizational incidents, daily operations, safety audits, and compliance activities.

3. Responsibilities

- **All Employees:** Accurate and timely recording and reporting of required information.
- **Supervisors/Managers:** Verification of documentation completion and compliance with standards.
- **Compliance Officer:** Regular audits and maintenance of confidentiality protocols.

4. Reporting Procedure

1. Identify the event or activity requiring documentation (e.g., incident, audit, safety check).
2. Complete the relevant standardized form or report template (see Section 8).
3. Submit the completed report to the assigned supervisor or designated recipient within 24 hours or as specified.
4. Follow-up on corrective actions, if required, and document outcomes.

5. Documentation Standards

Document Type	Required Elements	Format	Retention Period
Incident Report	Date, time, description, persons involved, actions taken	Incident Report Form	5 years
Safety Checklist	Date, location, completed by, findings, corrective actions	Checklist Template	3 years
Compliance Audit	Date, scope, auditors, findings, recommendations	Audit Report Template	5 years
Operational Log	Date, summary of activities, responsible personnel	Log Sheet	2 years

6. Record-Keeping and Storage

- All documentation must be stored in secure, designated locations (physical or digital) with access limited to authorized personnel.
- Electronic records must be backed up in compliance with IT policies.
- Dispose of records after the retention period following secure destruction protocols.

7. Confidentiality Protocols

- Confidential information in reports must be clearly marked and protected against unauthorized disclosure.
- Sharing of reports is restricted to personnel with a legitimate business need.
- Breaches of confidentiality must be reported immediately per policy.

8. Standard Forms and Templates

- Incident Report Form
- Safety Checklist Template
- Compliance Audit Report Template
- Operational Log Sheet

All current templates are available on the organization's shared drive or document management system.

9. Review and Continuous Improvement

- This SOP and all reporting/documentation forms must be reviewed annually or following significant incidents or regulatory updates.
- Staff feedback is encouraged to improve accuracy and efficiency.

10. References

- Applicable legal/regulatory requirements
- Internal policies on information security and data retention
- Compliance and audit standards