SOP: Documentation Requirements for Incident Details and Evidence Collection

Purpose: This SOP defines the **documentation requirements for incident details and evidence collection**, ensuring accurate, thorough, and timely recording of all relevant information related to incidents. It covers the proper methods for capturing evidence, maintaining chain of custody, completing incident reports, and storing documentation securely to support investigations, compliance, and future safety improvements.

1. Scope

This SOP applies to all employees, contractors, and third parties responsible for incident response, evidence collection, and documentation within the organization.

2. Responsibilities

- **Incident Response Team:** Responsible for collecting and documenting incident details and evidence.
- **Supervisors/Managers:** Ensure compliance with documentation procedures.
- **IT/Security Personnel:** Provide technical and forensic support for evidence preservation.

3. Incident Details Documentation Requirements

1. Use the official Incident Report Form (see template below) for all incidents.
2. Document the following information for each incident:
    - Date and time of incident detection and reporting
    - Location and system(s) affected
    - Type of incident (e.g., security breach, injury, system failure)
    - Names and contact details of individuals involved or witnesses
    - Detailed description of the incident (who, what, where, when, how)
    - Actions taken immediately and during response
    - Initial assessment of impact and severity
3. Ensure all entries are factual, time-stamped, and free from personal opinions or assumptions.

4. Evidence Collection Procedures

1. Identify and preserve potential evidence as soon as an incident is confirmed.
2. Collect evidence using approved methods:
    - Photographic/video documentation of physical scenes
    - Forensic imaging/cloning for digital evidence
    - Securing log files and relevant system data
    - Collecting witness statements (written or recorded)
3. Record the following for each item of evidence:
    - Description and unique identifier (e.g., evidence tag)
    - Date/time of collection
    - Name and signature of collector
    - Location where evidence was found
    - Condition and packaging details

5. Chain of Custody

1. Maintain a detailed chain of custody log for all evidence from collection through final disposition.
2. For each transfer, document:
    - Date and time of transfer
    - Parties transferring and receiving evidence (names, signatures)
    - Purpose of transfer
3. Keep evidence in secure, access-controlled storage at all times.

6. Storage and Security of Documentation

- Store all incident documentation and evidence logs in a secure, access-controlled repository (electronic or physical).

- Limit access to authorized personnel only.
- Maintain backups of electronic records in accordance with data retention policies.
- Do not alter or delete any records after they are finalized; corrections should be added as new entries with explanation and timestamps.

7. Incident Report Form Template

Field	Description
Incident Report Number	Unique identifier assigned by the reporting system
Date/Time Reported	Date and time the incident was reported
Location	Physical or system location(s) of the incident
Reported By	Name and contact details of the person reporting
Incident Description	Detailed account of what happened
Individuals Involved	Names, roles, and contact info of involved parties
Immediate Actions Taken	Details of steps taken in response
Evidence Collected	List and description of all evidence items
Chain of Custody Reference	Link to chain of custody log for each evidence item
Initial Impact Assessment	Preliminary evaluation of severity or impact
Reporter's Signature/Date	Authentication of report and timing
Reviewed By/Date	Supervisor or manager sign-off

8. Review and Updates

- This SOP will be reviewed annually or after any significant incident to ensure continued relevance and effectiveness.
- All updates must be documented, approved, and communicated to relevant personnel.

9. References

- Relevant regulatory, legal, and organizational compliance requirements
- Data retention and privacy policies
- Incident Response Policy