SWGDE/SWGIT Recommended Guidelines for Developing Standard Operating Procedures

Disclaimer:
As a condition to the use of this document and the information contained therein, SWGDE/SWGIT request notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE/SWGIT as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org and Chair@swgit.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE/SWGIT grant permission for redistribution and use of all publicly posted documents created by SWGDE/SWGIT provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE/SWGIT cover page containing the disclaimer.
2. Neither the name of SWGDE/SWGIT nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE/SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE/SWGIT encourage stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded in writing to secretary@swgde.org and Chair@swgit.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE/SWGIT logos or documents without written permission from SWGDE/SWGIT is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE/SWGIT work. This includes claiming oneself as a contributing member without actively participating in SWGDE or SWGIT meetings; claiming oneself as an officer of SWGDE or SWGIT without serving as such; claiming sole authorship of a document; use the SWGDE/SWGIT logos on any material and/or curriculum vitae.

Any mention of specific products within SWGDE/SWGIT documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE/SWGIT.

Recommended Guidelines for Developing Standard Operating Procedures

Introduction:

Standard Operating Procedures (SOPs) are agency unique documents describing the methods and procedures to be followed in performing routine operations. SOPs are essential to improve the quality and to implement uniform processes for conducting digital & multimedia evidence forensic tasks in a precise, accurate manner. SOPs should be task-based and written for each procedure conducted. They should be reviewed at least annually. The previously approved versions of an SOP should be retained for reference.

Scope:

SOPs should conform to agency-specific policies. Such policies may address document format, workflow, approval process, and tasks performed. SOPs may be stored separately, in one large collected manual, or organized by functional unit. For instance, a single manual may be more convenient, but having separate SOP documents may be more amenable to the discovery process. SOPs should contain all information necessary to perform the task being described. Individual agency needs and/or processes will dictate what information is necessary.

General Guidelines:

SOPs may include but are not limited to:

- The name of the SOP, effective date and/or other version control.
- The purpose and scope of the SOP.
- Definitions and abbreviations that are not commonly used or have a special connotation in the SOP. The source of these definitions should be cited.
- A list of equipment, materials and standards/controls.

    - **Note:** Since equipment and material lists are frequently updated, it may be beneficial to create a separate listing of this equipment. This will allow for a document that can be updated independent of the SOP.

    - Equipment calibration and similar preparatory steps, if applicable.
    - Any known limitations of the equipment, software or procedure.
    - A list of steps used in performing the task, including appropriate parameters or options to be used.
    - Appropriate references. This may include equipment manuals, other published procedures, journal references, etc.

- Any additional information/materials the examiner needs to be aware of that are not already included in the sections above, such as safety issues or operational precautions.
- Authorization and approval information.

Sample SOPs are provided for your reference. These are examples only and are not meant to be boilerplate.

Sample Standard Operating Procedure
Wiping Media
Version: Draft 1.0 (08/2003)
Version: Revised Draft 1.1 (02/2004)
Version: Revised Draft 2.0 (4/2004)

> **Note:** The sample standard operating procedures are given as an example only and are not meant to be used without revision.

Introduction/Scope:
This procedure applies to wiping media for hard disk drives and other digital media. This procedure applies to computer forensic examiners in this agency.

Purpose:
To completely erase, by overwriting, all data on digital media including both physical and logical structures.

Equipment:

X Media to be wiped
X Examination station
X ABC software wiping utility (current or appropriate version)

Definitions:
Wiping - To erase completely by overwriting all data on digital media including both physical and logical structures,

Calibration:
None

Limitations:
This procedure may not apply to all forms of media, such as tapes or diskettes.

Procedure:

1. Ensure the examination station is powered off.

2. Attach media to be wiped to examination station.

3. Power on the examination station.

4. Start wiping process utilizing appropriate software commands.

5. When process is complete, verify the media has been wiped.

6. Power off examination station.

7. Remove the media.

References:
ABC user manual for software wiping utility.

Notes:
Examiners should double check media before wiping to ensure no irreplaceable data will be lost.

History:

Revision	Date	Section	Change
1.1	01/05/2004	Notes	Spelling correction

This standard operating procedure has been approved for use.

Jane Doe
Approving Authority
Date

Note: The sample standard operating procedures are given as an example only and are not meant to be used without revision.

1. Do a visual inspection of the tape and cassette housing to

    a. Ensure housing is intact

    b. Inspect tape for damage (e.g., twisting, separation)

    c. If damage is found, take corrective action and document.

2. Enable any record-protection device (e.g., punch-out tab, slide record tab, remove record button).

3. Determine if the submitted tape is an original or a copy. If it is an original, proceed to Step 4. If it is a copy, contact the submitter and request that original tape be submitted, and terminate examination of the copy. If the copy is the best available, proceed with the examination.

4. Determine the make, model, and settings of the device used to record the submitted video, if possible. These settings may include the recording format and speed.

5. Select the appropriate playback device(s) to achieve optimal signal quality.

6. Using the selected devices and settings, review the submitted video to locate the pertinent segment(s).

7. Determine the appropriate playback speed for processing.

8. A time-base corrector may be used to stabilize the signal for playback and permit adjustment of video, chroma, pedestal levels, or other signals.

9. At the examiner's discretion, a working copy of the pertinent segment may be generated using an available analog or digital device.

10. The images may be enhanced using a number of processing operations that may include but are not limited to histogram equalization, multiframe

averaging, contrast and levels adjustments, and sharpening.

11. Once enhanced, the final images are output to appropriate media.

This standard operating procedure has been approved for use.

Jane Doe
Approving Authority
Date

History
SWGDE/SWGIT Recommended Guidelines for Developing Standard Operating Procedures

Revision	Issue Date	Section	History
1.0	11/15/04	All	Original Release
	04/10/06 Review Only	All	Review of document by SWGDE Forensics Committee. No revision necessary.
	9/27/2014 Admin Change Only	Disclaimer	Updated document with new SWGDE/SWGIT disclaimer. No changes to content and no version/publication date change.