Scientific Working Group on Digital Evidence

SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests 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 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.

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 grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE 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 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 encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.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 logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

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

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

SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers

Table of Contents

1. Purpose

The purpose of this document is to present a foundational framework on which to develop a Quality Management System (QMS) for Digital and Multimedia Evidence (DME) Forensic Science Service Providers (FSSP).

2. Scope

The intended audience includes any stakeholders interested in DME Quality Assurance. This document is limited to identifying the primary components of a QMS and is not intended to identify specific minimum requirements. Specific minimum requirements are addressed in current and future SWGDE work products.

3. Quality Management System Framework

The following components should be addressed via policies, processes, and procedures. The requirement for any of these components may be satisfied by referencing an existing organization policy and need not be re-specified in the DME QMS, if to do so would be redundant or create conflict.

A complete DME QMS will address the following topics (not listed in any order of precedence):

3.1 Employment Qualifications

Requirements based on individual FSSP specifications, functional roles, and job descriptions.

3.1.1 Position Description

Establish a detailed job description for all positions involved in laboratory operations (e.g., lab director, quality manager, analyst, forensic examiners or however named). For each position, identify the required:

- Roles and responsibilities;
- Physical capabilities;
- Technical knowledge, skills, and abilities;
- Definition of employees' commitment to job requirements.

3.1.2 Background Screening

Verify an applicant's background, including verification of:

- Minimum security requirements;
- Level and type of security clearance;
- Credit clearance/financial stability.

3.1.3 Education and Experience

Verify an applicant's education and/or experience, including verification of:

- High school diploma, undergraduate degree, graduate degree;
- Experience in lieu of education;
- Establish minimum job-related experience;
- Internship;
- Forensic experience from law enforcement or private sector;
- Additional specialized course(s) in forensics.

3.1.4 Pre-Employment Testing Process

Establish a testing program for potential employees that measures the employees' knowledge, skills, and abilities.

3.1.5 Record Keeping

Ensure records used in the hiring and pre-employment testing processes are maintained in a manner consistent with the policies of the FSSP.

3.2 Professional Development and Training

Address and document the individual's knowledge, skills, and abilities (KSA) through initial assessments and subsequent training and evaluation to meet FSSPs policy.

3.2.1 Initial Training

Plan for providing foundational training or verification of KSAs for new personnel.

- Perform an initial assessment of new personnel measured against FSSP-defined KSAs.
- Identify disparities between assessment and KSAs.
- Identify internal and external training based on assessment, according to the resources and requirements of the FSSP.
- Re-test new personnel to confirm the disparities have been addressed.

3.2.2 Mentorship

Provide for internal or external professional guidance to develop technical competency.

- Assign a mentor for each new employee (internal or external mentor).
- Develop a mentorship plan to identify achievable milestones during the mentorship process.
- Develop a review plan for mentee progress.

3.2.3 Competency Testing

Evaluate personnel's knowledge and abilities prior to performing independent forensic casework.

- Develop a plan to evaluate competency in each discipline the FSSP performs.
- Develop a progress plan for each examiner specific to the examiner's discipline(s) of testing.
- Document authorization memos for technical services.
- Develop a remediation process for competency falling below standards (e.g., additional training, mentoring, removal of discipline from examiner's authorized discipline).

3.2.4 Continuing Education and Training

Plan for providing continuing education and training for existing personnel to maintain competency in the technical procedures they conduct.

- Identify continuing education needs and resources.
- Develop a minimum policy for individual continuing education training.
- Develop a plan for providing continuing education and training for personnel.

3.2.5 Proficiency Testing

Evaluate personnel's ongoing performance.

- Develop a plan to address the frequency and type of testing required for each analyst.
- Analysts should undergo proficiency testing for each sub-discipline in which they conduct independent casework.
- Develop a remediation process for proficiency falling below standards (e.g., additional training, removal of discipline from examiner's authorized discipline).

3.2.6 Certification

Certify DME analysts in the sub-disciplines in which they conduct independent casework.

- Develop a plan for obtaining certifications related to the discipline(s) of each examiner.

3.2.7 Record Keeping

Maintain records used in the training, testing, and certification processes in a manner consistent with the policies of the FSSP.

3.3 Laboratory Standards

Establish a working environment for acquiring and/or processing digital and multimedia evidence in a forensically sound manner.

3.3.1 Personnel

Define roles, responsibilities, and/or job descriptions relevant to the technical services personnel are authorized to provide.

- Define roles and responsibilities relevant to authorized work.
- Create an organizational chart.
- Establish job performance expectations and a performance review plan.

3.3.2 Work Environment

Establish standards for health, safety, security, and access control.

3.3.2.1 Laboratory Environment

- Establish logical and physical access permissions/policies/control points.
- Establish access logging and auditing system policy and procedure.
- Document a policy for visitors.
- Establish a security system policy (lab or building system).
- Establish a disaster recovery and business continuity plans for lab.
- Address power and ventilation needs.
- Establish environment controls to ensure evidence storage.
- Establish a hazardous materials policy.

3.3.2.2 Field Environment

- Develop quick response plans.
- Develop safety policies and procedures (e.g., two-person teams).

3.3.3 Evidence Management

Establish a system for managing evidence from intake through final disposition

- Establish policies and procedures for:
  - Chain of custody (e.g., unique identifiers, initials, handling);
  - Laboratory inventory management system;
  - Retention, preservation, and disposition;
  - Secured storage.
- Establish a policy for electronically stored information (ESI).

3.3.4 Tools, Techniques, and Procedure

Establish a system for identifying tools, techniques, and procedures used to perform forensic examinations. This includes testing of equipment and software, and testing and documentation of nonstandard methods.

- Define the category of tools.
- Establish a testing policy.
- Establish a policy for maintaining inventory lists.
- Define sequencing/workflow for jobs.
- Establish a policy to approve methods and techniques.
- Consider best practices (e.g., SWGDE, ASTM International).

3.3.5 Equipment Maintenance

Establish guidelines for equipment maintenance to ensure proper performance.

- Establish a policy for equipment maintenance.
- Define a policy for maintaining records.
- Establish a policy for "out of service" repairs and return to service.
- Develop a process for ordering, invoicing, and purchasing.
- Define a policy for firmware upgrades.
- Maintain reference materials (e.g., vendor manuals and warranties).

3.3.6 Standard Operating Procedures (SOP)

Develop written documentation for DME examinations.

- Establish standard operating procedures (SOPs).
- Consider accepted best practices and industry standards.
- Define laboratory requirements.
- Define approved methods/techniques.
- Define a policy for deviations.
- Create written "how to" for examinations.

3.3.7 Technical/Peer Review

Ensure reviews are conducted by a second qualified individual of reports, notes, data, conclusions, and other documents, including reviewing for consistency with laboratory technical policies.

- Set policy for the percent of casework to be reviewed.
- Establish a procedure for authorizing an employee to conduct reviews.
  - Define qualifications.
  - Document authorization.
  - Ensure the reviewer is separate from the analyst performing the exam.
- Define the scope of the reviews.
- Create standard technical review criteria.

3.3.8 Administrative Review

Ensure casework is reviewed for editorial standards and consistency with laboratory administrative policies.

- Set policy for the percent of casework to be reviewed.
- Define the scope of the reviews.
- Create standard administrative review criteria.

3.3.9 Document Control

Establish a process for controlling the QMS documents.

- Establish a process for the development, review, and approval of QMS documents.
- Establish a document storage system (e.g., electronic vs. paper).
- Establish procedures for the use and organization of QMS documents.
- Define procedures for identifying current documents and archived versions.

3.3.10 Audits of QMS

Perform periodic reviews of the QMS policy and procedures for relevancy and continued improvement.

- Define the scope of audit (i.e., internal review of technical records, methods, and laboratory personnel compliance with the quality system).
- Define the scope of the management review (i.e., internal review of the quality system as a whole by laboratory management).
- Define audit frequency and scheduling.
- Identify personnel authorized to conduct audit.
- Establish policy for maintaining records of audits and the cycle for retention.

3.3.11 Complaints and Corrective Actions

Establish a process to address internal and external concerns.

- Establish a policy for addressing:
  - customer and employee concerns/suggestions,
  - deficiencies identified in the quality system,
  - issues identified during audits/review of casework, and
  - internal process feedback and continued improvement.
- Develop preventative action process.
- Document and implement preventative and corrective actions based on the identified concerns.

3.3.12 Disclosure of Information

Establish a procedure detailing how case related information is released.

- Establish a policy for release of case information (e.g., customers, FOIA, legal requests).
- Establish a policy for the release of laboratory or personnel information.

3.3.13 Testimony Monitoring

Establish procedures to track and assess testimony.

- Establish a policy for documenting and reviewing examiner testimony.
- Establish procedures for providing examiner feedback of testimony review.

3.4 Case Workflow Guidelines

Establish guidelines for case lifecycle, from intake to final disposition.

3.4.1 Service Request

Establish procedures for how service requests are submitted, reviewed, and accepted or declined.

- Develop a service intake process, which includes:
  - a record of the requesting party & contact information,
  - delivery parameters, and
  - defined and confirmed scope of work.
- Provide submission instructions to customers.
- Establish a process for approval, and criteria for rejection, of requests.
- Identify appropriate legal authority.
- Define procedures for scope modification and resubmission/review.

3.4.2 Evidence Handling

Establish procedures for maintaining the integrity of the evidence during examination.

- Establish procedures for handling evidence during examinations, which includes:
  - properly identifying derivative evidence,
  - securing evidence, and
  - logging evidence interaction/transfer (e.g., chain of custody).
- Establish access controls for evidence storage.

3.4.3 Examination

Establish technical procedures related to requested services.

- Follow SOPs for requested service.
- Follow procedures when deviating from approved methods.
- Maintain controlled work environment.
- Follow procedures for technical and administrative reviews.

3.4.4 Documentation

Documentation may include service request, legal authority, chain of custody, examination notes, reporting of results, findings, conclusions, and technical/administrative reviews.

- Maintain appropriate documentation for tracking, recording, and validating activity associated with case management.

4. References and Resources

[1] *Standard Guide for Education and Training in Computer Forensics*, ASTM Standard E2678 - 09, 2014.

[2] National Research Council, Committee on Identifying the Needs of the Forensic Sciences Community, "Strengthening Forensic Science in the United States: A Path Forward," Document No.: 228091. Award Number: 2006-DN-BX-0001, August 2009. [Online]. https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

[3] National Commission on Forensic Science, "Views of the Commission Regarding Critical Steps to Accreditation," March 22, 2016. [Online]. https://www.justice.gov/ncfs/file/839701/download

[4] Scientific Working Group on Digital Evidence, "SWGDE Core Competencies for Forensic Audio". [Online]. https://www.swgde.org/documents

[5] Scientific Working Group on Digital Evidence, "SWGDE Core Competencies for Mobile Phone Forensics,". [Online]. https://www.swgde.org/documents

[6] Scientific Working Group on Digital Evidence, "SWGDE Digital & Multimedia Evidence Glossary". [Online]. https://www.swgde.org/documents

[7] Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology, "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence". [Online]. https://www.swgde.org/documents

SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers

History

Revision	Issue Date	Section	History
1.0 DRAFT	2017-01-12	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2017-02-21	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2017-06-22	All	Rewrites made to all sections of the initial draft. SWGDE voted to re-release as a Draft for Public Comment.
1.0 DRAFT	2017-07-11	All	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.0	2017-08-24	3.1.1; 3.3.3	Minor edits made for clarification purposes. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2017-09-25		Formatted and published as Approved Version 1.0.