BEST PRACTICES FOR DIGITAL EVIDENCE LABORATORY PROGRAMS

PART 1 – Recommendations for Education and Training

SECTION 1 – INTRODUCTION

1.1 Recommendations listed below are intended to apply to any examiner who:

1.1.1 Forensically examines and analyzes digital evidence or related materials, or directs such examinations to be done.

1.1.2 As a consequence of such examinations, signs reports for legal and administrative proceedings and provides testimony as required.

SECTION 2 - MINIMUM RECOMMENDATIONS FOR EDUCATIONAL REQUIREMENTS (for a further explanation of personnel/duties see section 7)

2.1 TECHNICIAN/ASSISTANT

2.1.1 Have education, skills, and abilities commensurate with their responsibilities.

2.1.2 Have on-the-job training specific to their position.

2.2 EXAMINER

2.2.1 An examiner should have at least a baccalaureate degree in criminalistics, science, or a related field of study. An examiner without a baccalaureate degree, should meet one of the following conditions:

2.2.1.1 Sixty semester hours of college level study to include course work in related fields of study;

<u>OR</u>

2.2.1.2 A minimum of two (2) years practical experience in the area of digital evidence examination, and have demonstrated competency following the completion of a formal, documented training program.

2.3 TECHNICAL MANAGER/LEADER

2.3.1 Meet all the requirements of an examiner.

2.3.2 Have a minimum of two (2) years of experience as an examiner in the forensic analysis of digital evidence.

2.3.3 Exhibit knowledge necessary to evaluate results and conclusions.

SECTION 3 - CONTINUING PROFESSIONAL DEVELOPMENT

3.1 All personnel have an ongoing responsibility to remain current in their field. In addition, agencies should provide support and opportunities for continuing professional development. The recommended minimum continuing professional development requirements for personnel are:

3.1.1 Forty annual hours of training relevant to the examiner's responsibilities. All training, once completed, must be documented. The training can be provided from a variety of sources, including but not limited to:

3.1.1.1 Courses taught at the post-secondary educational level

3.1.1.2 Courses taught by vendors

3.1.1.3 In-service training conducted by the employer

3.1.1.4 In-service training taught by external provider

3.1.1.5 Attendance at workshops and participation in relevant scientific meetings or conferences.

3.1.2 To maintain membership in a field related professional organization.

SECTION 4 - MINIMUM RECOMMENDATIONS FOR TRAINING PROGRAMS

Agencies should set their training programs to meet their needs as they relate to the types of casework encountered, equipment available, and the level of competency of trainees.

4.1 A written training program, approved by the agency's management, focusing on the development of the theoretical and practical knowledge, skills and abilities necessary to perform duties assigned, includes:

4.1.1 A training syllabus including descriptions of the knowledge and skills required by an examiner (specific topic areas), milestones of achievement, and methods of testing or evaluating competency.

4.1.2 Documented standards of performance and a plan for assessing theoretical and practical competency against these standards (e.g. written and/or oral examinations, critical reviews, mock casework, etc., per topic area).

4.1.3 A period of supervised case work that is representative of the type of case work required to be performed.

4.1.4 Documentation verifying that the trainee has achieved the desired competence per specific topic area.

4.2 Topic areas in the training program should include, as a minimum, the following:

4.2.1 Relevant background information on digital evidence, such as:
Hardware
Software
Operating systems
Relevant applications
File identification
Relevant media (digital/analog)
File systems

4.2.2 Techniques, methodologies and equipment utilized in the examination of digital evidence and related materials, such as:
Forensic analysis procedures
Best practices (technical procedures)
Standard operating procedures

4.2.3 Quality assurance, such as:
Quality assurance *(for consistency within the forensic community)*
Technical writing *(for concise, clear reports)*
Presentation skills *(for the explanation of information)*
General forensic principles and practices *(for base of knowledge)*

4.2.4 Expert/Court testimony and legal requirements, such as:
Public speaking *(to build confidence in speaking situations)*
Testimony skills *(to establish a comfort level for testimony)*
Admissibility (Daubert) Hearing Testimony *(for issue awareness)*
General criminal justice *(to understand authority and result of examinations)*
Basic crime scene management *(to understand scene and evidence complexity)*

4.2.5 Agency policies and procedures as they relate to the examination of digital evidence and related materials, such as:
Safety *(for the purpose of risk management and personal safety)*
Security *(to preserve chain of custody)*
Ethics *(to conform to a standard of integrity)*
Evidence handling *(to preserve integrity of evidence)*

Training documentation *(to demonstrate compliance)*

4.3 An individual providing training must have the knowledge, skills, and abilities in the subject area for which they are providing instruction.

SECTION 5 - MINIMUM DOCUMENTATION/REFERENCE MATERIAL AVAILABLE TO AN AGENCY PERFORMING DIGITAL EVIDENCE EXAMINATIONS

5.1 Documentation/reference resources should be available and accessible to examiners in hard copy or electronic form, such as:

5.1.1 College/university level textbooks as references to theory and practice in key subject areas, e.g. hardware, software, and operating systems.

5.1.2 Reference literature pertaining to digital evidence.

5.1.3 Operation and maintenance manuals for all hardware and software available for use by the examiner.

5.1.4 Relevant publications and periodicals.

5.1.5 Agency quality manual and standard operating procedures.

5.1.6 Relevant jurisdictional legislation (e.g., statutes and case law relating to digital evidence, etc.).

5.1.7 Internet access.

PART 2 – Recommendations for Quality Assurance Guidelines

SECTION 6 - INTRODUCTION

A digital evidence program should incorporate quality assurance. It is the goal of these guidelines to provide a framework of quality management in the processing of digital evidence, including evidence handling, management practices, analyses, and reporting.

6.1 QUALITY MANAGEMENT SYSTEM

A documented quality management system must be established and maintained.

6.1.1 The personnel responsible must be clearly designated and shall have access to management responsible for organizational policy.

6.1.2 The quality management system must cover all procedures and reports associated with evidence.

SECTION 7 - PERSONNEL

7.1 JOB DESCRIPTION

The job descriptions for all personnel should include responsibilities and duties.

7.2 DESIGNATED PERSONNEL AND RESPONSIBILITIES

An individual (however titled) may be responsible for more than one of the following duties:

7.2.1 Quality Assurance Manager: A designated person who is responsible for maintaining the quality management system (including an annual review of the program) and who monitors compliance with the program.

7.2.2 Health & Safety Manager: A designated person who is responsible for maintaining a Health and Safety program (including an annual review of the program) and who monitors compliance with the program.

7.2.3 Operational Manager: A designated person who has the overall responsibility and authority for the operations of the unit.

7.2.4 Technical Manager/Leader: A designated person who has the overall responsibility and authority for protocols and analytical methodologies.

7.2.5 Examiner: A designated person who:

7.2.5.1 Examines and analyzes digital evidence or related materials, or directs such examinations to be done.

7.2.5.2 Signs reports for legal and administrative proceedings.

7.2.6 Technician/Assistant: A person who works with evidence, but typically does not issue reports for court purposes.

7.3 QUALIFICATIONS/EDUCATION

The agency should articulate its minimum qualifications, training and education requirements consistent with those stipulated in Part 1 of this guide.

7.4 TRAINING

The agency must establish and document a training program and qualifying procedure for all technical personnel. A written training program, approved by management, should focus on the development of the theoretical and practical knowledge, skills and abilities necessary to examine digital evidence and related materials as enumerated in Part 1 of this guide.

7.5 MAINTAINING QUALIFICATIONS

The agency must establish and document the minimum continuing professional development requirements for all technical personnel as enumerated in Part 1 of this guide.

SECTION 8 - PHYSICAL PLANT

8.1 FACILITY REQUIREMENTS

8.1.1 The facility shall provide adequate safety and security for personnel and operations.

8.1.2 The facility must meet required health and safety standards.

8.1.3 The facility must contain adequate space to perform required analytical functions and prevent alteration/damage to evidence.

8.1.4 A fume hood may be needed when the physical evidence poses a health and/or safety hazard to the examiner (e.g., for digital evidence that was seized in a clandestine drug lab, a crime scene containing biological materials, or other potentially hazardous environments). It must be properly maintained and monitored according to an established schedule.

8.1.5 A facility should maintain general cleanliness.

8.1.6 Facilities must be designed to ensure the proper safe-keeping of evidence, data, and records to protect from loss, cross-transfer, contamination and/or deleterious change. Appropriate precautions should be taken with regard to electrostatic discharge, electrical and magnetic fields to ensure the integrity of the digital evidence.

8.1.7 Appropriately secured storage areas must be provided.

SECTION 9 - EVIDENCE CONTROL

The unit shall have and follow a documented evidence control system to ensure the integrity of physical and digital evidence.

9.1 RECEIVING AND IDENTIFYING EVIDENCE

The unit must maintain records of requests for service and of the respective items of evidence. A unique identifier must be assigned to each case file or record. This file or record must include at least the following:

9.1.1 The request for service document or a copy thereof.

9.1.2 The identity of the party requesting the service and the date of the request.

9.1.3 A description of items of evidence submitted with each having a unique item identifier.

9.1.4 The identity of the person who delivers the evidence, along with the date of submission. For evidence not delivered in person, descriptive information regarding the mode of delivery and tracking information.

9.1.5 The chain of custody record.

9.1.6 Documentation of communication with the submitter.

9.2 INTEGRITY OF EVIDENCE

Evidence must be properly secured and labeled in accordance with the agency's digital evidence handling policy. Appropriate storage conditions shall ensure that the digital evidence is not altered or lost. All actions taken with regard to the digital evidence will be documented. A description of the evidence shall be compared to documentation prior to examination. Any irregularities should be identified at this time, documented in the case file and the submitter promptly informed.

9.3 STORAGE OF EVIDENCE

Access to the evidence storage area must be granted only to persons with authorization. Access shall be controlled.

9.4 DISPOSITION OF EVIDENCE

Records must be kept regarding the disposition of all items of evidence.

9.5 DOCUMENTATION PROCEDURES

All records, such as results of examinations, measurements, notes, calibrations, spectra and reports, shall be retained in a secure fashion.

SECTION 10 - EXAMINATION PROCEDURES

10.1 PROCEDURES FOR DIGITAL EVIDENCE EXAMINATION

10.1.1 The unit shall have and follow written examination procedures.

10.1.2 Work practices shall be established to prevent contamination of evidence during examination procedures.

10.1.3 The unit shall monitor the examination procedures using appropriate controls and traceable standards.

10.1.4 Examination procedures must be validated in compliance with Section 14.

10.2 QUALIFICATION OF REFERENCE MATERIALS

10.2.1 The credibility of reference material should be confirmed prior to their first use.

10.2.2 Unconfirmed reference materials must be qualified prior to use.

10.2.3 All qualifications must be documented to include the name of the individual who performed the qualification and the date of qualification.

SECTION 11 - EQUIPMENT PERFORMANCE

‘Equipment’ in this section refers to the non-evidentiary hardware and software the examiner utilizes in the course of an examination.

11.1 Equipment must be monitored and documented to ensure proper performance is maintained.

11.2 Only suitable and properly operating equipment shall be employed.

11.3 The manufacturer's operation manual and other relevant documentation for each piece of equipment should be readily available.

SECTION 12 - DOCUMENTATION, REPORTS, AND REVIEW

12.1 DOCUMENTATION

12.1.1 Documentation must contain sufficient information to allow a peer to evaluate case notes and interpret the data.

12.1.2 Evidence handling documentation should include: chain of custody, the initial count of evidence to be examined, information regarding the packaging and condition of the evidence upon receipt by the examiner, a description of the evidence, and communications regarding the case.

12.1.3 Examination documentation should include items such as: observations, examination processes and results, and supporting charts, graphs, and spectra generated during an examination.

12.1.4 Documentation must be preserved according to written agency policy.

12.2 REPORTS

12.2.1 Reports issued by the unit must address the requests of the submitter.

12.2.2 Reports should include:

a. Identity of the reporting agency
b. Case identifier or submission number
c. Identity of the contributor
d. Date of receipt
e. Date of report
f. Descriptive list of submitted evidence
g. Identity of examiner
h. Results/Conclusions

12.2.3 Written procedures for the release of case report information should be established.

12.3 REVIEW

12.3.1 The agency must have a written policy establishing the protocols for technical and administrative review.

12.3.2 The agency must have a written policy to determine the course of action should an examiner and reviewer fails to agree.

SECTION 13 - COMPETENCY AND PROFICIENCY TESTING

Each agency should participate in at least an annual proficiency testing program and should have written protocols for testing the competency and proficiency of its examiners.

13.1 COMPETENCY TESTING

13.1.1 Units will monitor and document the competency of their examiner trainees and technical support personnel prior to assumption of casework responsibilities.

13.1.2 Competency testing samples should be representative of the unit's normal casework.

13.1.3 Competency testing must comply with the unit's standard operating procedures and other protocols.

13.2 PROFICIENCY TESTING - INTERNAL

13.2.1 Each examiner shall be proficiency tested annually in each sub-discipline in which casework is performed.

13.2.2 The proficiency testing samples should be representative of the examiner's normal casework.

13.2.3 The test examination must comply with the unit's standard operating procedures.

13.3 PROFICIENCY TESTING - EXTERNAL

13.3.1 Each unit shall be proficiency tested annually in order to verify the unit's performance.

13.3.2 The proficiency testing samples should be representative of the unit's normal casework.

13.3.3 The test examination should follow the unit's standard operating procedures.

13.3.4 The proficiency tests shall be obtained from approved test providers where available.

SECTION 14 - VALIDATION

14.1 Validation is required to demonstrate the examination procedures and tools are suitable for their intended purpose.

14.1.1 Minimum acceptability criteria should be described along with means for demonstrating compliance.

14.1.2 Validation documentation is required.

SECTION 15 - INTERNAL AUDITS

15.1 Audits should be conducted at least once a year.

15.2 Records of each audit must be maintained and should include the scope, date of the audit, name of the person(s) conducting the audit, findings, and corrective actions taken, if necessary.

SECTION 16 - DEVIATIONS AND DEFICIENCIES

In the course of examining digital evidence and related materials, the unit may experience results that are anomalous in some manner. Each unit must have a written policy to deal with deviations and deficiencies.

16.1 As used in this guide, a deficiency is any erroneous examination result or interpretation, or any unapproved deviation from an established policy or procedure in an examination.

16.2 As used in this guide, a deviation is a departure from the established policies and procedures.

Comment: In developing policy the following may be considered: a requirement for immediate cessation of the activity or work of the individual or tool involved, if warranted by the seriousness of the deficiency, as defined in the written policy; a requirement for administrative review of the activity or work of the individual involved; a requirement for evaluation of the impact this deficiency may have had on other activities of the individual or other examiners; a requirement for documentation of the follow-up action taken as a result of the review; a requirement for communication to appropriate employees of any confirmed deficiency which may have implications for their work.

SECTION 17 - HEALTH AND SAFETY

The agency must have a documented health and safety program in place to meet the needs of the unit.

17.1 HEALTH AND SAFETY REQUIREMENTS

17.1.1 All personnel should receive appropriate health and safety training.

17.1.2 The digital evidence unit shall operate in accordance with agency policy and comply with any relevant statutory regulations.

17.1.3 Health and safety manual(s) shall be readily available to all personnel.

SECTION 18 - DOCUMENTATION

18.1 In addition to casework documentation the unit should maintain documentation on the following topics:

a. Test methods/procedures for digital evidence examination.

b. Reference materials (including source and qualification).

c. Evidence handling protocols.

d. Equipment calibration and maintenance.

e. Equipment inventory (e.g. manufacturer, model, serial number, acquisition date).

f. Proficiency testing.

g. Personnel training and qualification.

h. Quality assurance protocols and audits.

i. Health, safety and security protocols.

j. Validation data and results.

PART 3 – Recommended Procedures for Digital Forensic Examinations

The following information is provided as guidance for the development of agency Standard Operating Procedures (SOP). The SOP should address each of the following elements:

SECTION 19 – REVIEW THE REQUEST FOR SERVICE/EXAMINATION

19.1 Ascertain legal authority to perform the requested examination. The examiner will be provided with the legal authority that allows him/her to examine digital evidence. Examples of such authority include: consent to search by owner, subpoena, search warrant, or other legal authority.

19.2 Review documentation provided by the requestor to determine the processes necessary to complete the examination.

SECTION 20 – RECEIPT OF EVIDENCE PROTOCOL

20.1 Maintain chain of custody per established agency standard operating procedures for handling digital evidence.

20.2 Coordinate with the investigator and/or other forensic examiners when other forensic examinations may be required. Specifically, the order in which these forensic examinations will be conducted should be determined prior to any examination. (e.g. latent print analysis, DNA analysis, hair fiber analysis)

SECTION 21 - CONDUCT PHYSICAL INSPECTION OF ITEMS PRESENTED FOR DIGITAL EXAMINATION

21.1 Inspect and document the evidence received. Note condition of items received and any exceptions between the inventory of items received and the evidence reviewed by the examiner.

21.2 Assess the power needs for devices with volatile memory. Follow agency policy for the handling of these devices.

SECTION 22 – PREPARATION FOR EXAMINATION

22.1 The examiner should maintain evidence integrity, and will document any exceptions.

22.2 Establish conditions to prevent the possibility of data contamination.

SECTION 23 – CONDUCT EXAMINATION

23.1 Document evidentiary settings and configurations, if possible.

23.2 Extract digital information necessary to meet requirements of the examination.

23.3 Analyze and/or interpret the extracted digital information.

SECTION 24 – DOCUMENT THE EXAMINATION

24.1 The documentation must contain a sufficient level of detail such that another competent examiner could reproduce the same extracted results.

24.2 Reports issued must meet the requirements of the agency.

SECTION 25 – QUALITY CONTROL

25.1 Adhere to the agency's Quality Control procedures which should include:

25.1.1 Technical/Peer Review.

25.1.2 Administrative Review.

SECTION 26 – ISSUE REPORT

26.1 The report must be signed by the examiner.

SECTION 27 – DISPOSITION OF EVIDENCE

27.1 Adhere to organization's evidence disposition policy.

GLOSSARY

Administrative Review
A procedure used to check for consistency with laboratory policy and for editorial practice. (ASCLD/LAB)

Audit
A review conducted to compare the various aspects of a laboratory's performance with a standard for that performance. (ASCLD/LAB)

Digital Evidence
Information of probative value stored or transmitted in binary form. (SWGDE)

Digital Evidence Examiner (Examiner)
An individual responsible for the duplication, extraction and/or analysis of information from digital evidence, generation of work product, writing reports, and testifying in legal and administrative proceedings. (SWGDE)

Qualification Testing
Process to provide sufficient confidence that reference materials utilized are valid.

Quality Assurance
Those planned and systematic actions necessary to provide sufficient confidence that a laboratory's product or service will satisfy given requirements for quality. (ASCLD/LAB)

Reference Materials
As used in this document, this refers to items such as published literature, hardware and software documentation, hash sets, header sets, etc. (SWGDE)

Technical/Peer Review
An evaluation of reports, notes, data, and other documents to ensure an appropriate and sufficient basis for the scientific conclusions. This review is conducted by a second qualified individual. (In accordance with ASCLD/LAB)

Validation
The process of performing a set of experiments which establish the efficacy and reliability of a technique or procedure or modification thereof. (ASCLD/LAB)