State of North Carolina

Department of the Secretary of State

Information Technology Division

Digital Forensics Laboratory

Administrative Procedures Manual

APM-Lab

Reauthorization: ACappadonia 4/1/2019

Supersedes DFL-APM February 14, 2019
Version 3.1
Destroy Previous Editions
Distribution: All printed copies – Uncontrolled
Document Source: http://sosnet/IT Auth: ACappadonia

Ashley L. Cappadonia

Digitally signed by Ashley L. Cappadonia
Date: 2019.04.01 15:53:33 -04'00'

Table of Contents

Section 1.0 Scope 4

Section 2.0 Definition of Terms 5

Section 3.0 Annual Quality Audits 6

Section 4.0 Case File Review 7

Section 5.0 Certification 9

Section 6.0 Corrective and Preventive Action 10

Section 7.0 Document Control 13

Section 8.0 Equipment Records/Documentation 16

Section 9.0 Evidence Handling and Case Management 17

Section 10.0 Exceptions 22

Section 11.0 Inventories and Inspections 23

Section 12.0 Laboratory Case Record Contents 24

Section 13.0 LIMS Business Practices 28

Section 14.0 Management Continuity 29

Section 15.0 Management Reviews 30

Section 16.0 Proficiency Testing 32

Section 17.0 Quality and Technical Records 33

Section 18.0 Resolution of Complaints 34

Section 19.0 Review of Requests 35

Section 20.0 Services and Supplies 36

Section 21.0 Testimony Review 37

Section 22.0 Training Programs 38

Section 23.0 Validations and Performance Checks 40

Section 24.0 Appendix 41

1-0. SCOPE

A. The Administrative Procedures Manual (APM) describes policies and procedures not otherwise covered in the DFL Standard Operating Procedures or the Quality Manual.

B. The APM provides guidance in a number of administrative areas outside of normal laboratory operations, and is centered primarily on personnel guidance with day-to-day matters such as (but not limited to) certifications and proficiency testing.

C. This document outlines the policies and procedures for execution of various digital forensic laboratory tasks, and establishes a foundation for intra-agency cooperation using agency infrastructure and other management tools. Some unique situations may dictate variations in the procedures contained in this document. In these cases, common sense and prudent judgment must be used to ensure effective management of agency resources. Safety must always be a primary concern.

2-0. Definition of Terms. Below is a list of terminology, abbreviations, and general definitions commonly used or related to digital forensics:

A. 'SOSNET' – The N.C. Secretary of State intranet. Found at http://sosnet
B. Memorandum of Understanding (MOU) – An approved agreement with another organization or agency that may define DFL activities or case-work in support of that agency's incident or case. MOUs may contain provisions and restrictions that supersede those found in this document. MOUs should be on file with the General Counsel.
C. Qualified – DFL staff meets all agency requirements to work cases independently.
D. Retention – The length of time documentation or media must be maintained by the lab. There are multiple retention times affecting different types of documentation and media.
E. Electronically Controlled Document – Documents in an electronic format that are regulated to ensure that they are adequate, approved for use and the correct current version of the document.
F. Preventive Action Request (PAR) – Document detailing a course of action to prevent nonconformities from occurring, and to monitor its effectiveness.
G. Case Report – Reports that contain information regarding the examinations conducted and any information necessary for the interpretation of the examination results.
H. Case File – The file folder holding the case record.

3-0. Annual Quality Audits

A. The Digital Forensics Lab Manager will conduct an annual quality audit of the Digital Forensic Laboratory to by October 15th each year or sooner if deemed necessary. The Digital Forensics Lab Manager or designee may utilize a Quality Assurance Committee to assist in the audit process. The audit committee will use a checklist when conducting the annual quality audit. All quality audits should include the following:
    a. Staff's awareness of the quality manual
    b. Analytical procedure selection, control and validation
    c. Control of standards
    d. Equipment performance check and maintenance records
    e. Adequacy of case reports and notes and their disposition (only those case files completed since the last audit by current Lab analyst)
    f. Evidence handling procedures
    g. Proficiency testing
    h. Training and competency records of case-working members
    i. Handling of technical deficiencies and remedial action
    j. Laboratory orderliness and health and safety measures
    k. Review of testimony monitoring
    l. Review of new procedures
B. The Digital Forensics Lab Manager and Quality Assurance Committees must follow the laboratory's requirements for accessing case files.
C. Upon completion of the quality audit, the Deputy Secretary-IT will be briefed by the Quality Manager or designee as to the preliminary findings. Any issues unable to be corrected during the audit must be documented on the Quality Audit Report. The area of activity audited, the audit findings and corrective actions that arise from them shall be documented. Those findings that require corrective actions will follow the Administrative Procedure for Corrective and Preventive Actions.
D. A copy of the Quality Audit Report Form, including the checklist and a summary of any findings, will be provided to the Deputy Secretary-IT by October 15th of the audit year. The Deputy Secretary-IT will provide the Quality Manager with a response to the audit. The Quality Manager will be the final arbitrator of any disagreement on findings in consultation with the Deputy Secretary-IT.
E. Retention: Quality audit documentation will be maintained by the Quality Manager for at least five years.

4-0. Case File Review

A. Administrative review will be conducted on all completed case files, and technical casework review will be conducted on ALL of completed case files except for reports that do not include analytical conclusions, but only administrative information such as:
   a. Service request(s) un-worked

B. Administrative review will ensure the completeness and correctness of the reports issued and will be conducted by a member other than the author of the report. The review will include a check for consistency with policy and editorial correctness. This includes, but is not limited to, a review of the report and case record for:
   a. Spelling
   b. Grammar
   c. case number and initials on appropriate pages
   d. (see Administrative Procedure on Laboratory Case Record Contents, Management and Retention)
   e. descriptions of evidence and seals

C. Technical casework review will be conducted by a member other than the author or co-author of the report and will include a thorough review of bench notes, data, photographs and other documents that form the basis for the conclusions. At a minimum, technical reviews will include a review of all examination records and reports to ensure the following: conformance with Digital Forensic Laboratory technical procedures and laboratory policy and procedures; accuracy of the report; that the data supports the results and/or conclusions in the report; that associations are properly qualified in the report; and that the report contains all the required information. If any additional requirements exist, they are detailed in the respective discipline standard operating procedures. The member(s) conducting an administrative review and/or technical casework review will ensure that these actions are documented.

D. The Digital Forensics Lab Manager will ensure that members with technical knowledge in the examination area or testing method that is sufficient to ensure compliance with all discipline procedures and/or protocols, correct conclusion(s), reporting procedures and evidence handling policy and procedure, conduct the technical casework review. At a minimum, the member conducting and signing the technical casework review must be or have received specialized training in digital forensics.

Supersedes DFL- APM February 14, 2019
Version 3.1
Destroy Previous Editions
Distribution: All printed copies – Uncontrolled
Document Source: http://sosnet/IT Auth: ACappadonia

E. Technical casework review does not shift the responsibility for the forensic findings to the reviewer, but the reviewer is responsible to ensure that the documentation does reflect adequate basis for the conclusion.

F. Administrative deficiencies such as obliterations, strikeouts, or opaque correction fluid will be reported to the Deputy Secretary-IT if recurrent in nature.

G. Technical discrepancies will immediately be referred to the Digital Forensics Lab Manager who will follow the policy and procedures as detailed in the Administrative Procedure for Corrective and Preventive Action.

H. Each case-working member will proofread their reports ensuring the report reflects accurate information prior to submitting for review

5-0. Certification

A. Crime Laboratory Analyst Certification
   a. Digital (computer) Forensic Analysts must attain lab certification prior to conducting independent casework.
   b. Certification will be attained upon successful completion of a Digital Forensic analyst training program.

B. Certification in Computer Forensics
   a. Analysts certified in Computer Forensics must maintain certification in that area by independently completing a minimum of five (5) service requests and at least one proficiency test per major area per calendar year.

C. Any changes to the requirement of cases worked per discipline or category of testing must be submitted to the Deputy Secretary-IT for approval.

D. A member who was previously certified by NC Secretary of State DFL in Digital Forensics, but has not completed the minimum number of examinations in that area during the calendar year must be assessed prior to resuming independent casework.

E. Authorization to Operate Equipment
   a. The certification for computer forensic analysts will include authorization to operate items of equipment significant to the discipline

6-0. Corrective and Preventive Action

A. Corrective Action

a. *All* discrepancies and occurrences of non-conforming work or departures from the policies and procedures of the management system or technical operations will be evaluated and investigated *beginning with a root cause analysis* and they shall be properly noted, reported and promptly reviewed. Discrepancies will be evaluated prior to any changes or modifications in the work product or the issuance of any report; in keeping with best practices, this evaluation shall begin with a root cause analysis.

B. The laboratory member is responsible for his/her work product including technical review and verification. When necessary, the Digital Forensics Lab Manager will secure all notes, analytical work products and case files when an apparent discrepancy is noted, that has not been detected in the normal quality system activities. All casework for the examiner will be halted. Analytical documentation will be thoroughly reviewed to determine what caused the discrepancy. A Quality Assurance Review (QAR) form will be filled out and the Digital Forensics Lab Manager will determine if further action is necessary. If warranted, the Digital Forensics Lab Manager will then forward the form electronically to the Deputy Secretary-IT. Once a determination is made as to whether or not a Corrective Action Request (CAR) will be issued, the QAR will be printed and signed by the appropriate parties. Confirmation that a return to compliance has been achieved will be done by analyzing reference samples where appropriate. When necessary, a review of all casework relevant to the discrepancy will be performed to determine if the discrepancy is an isolated incident. Notification will be made to the investigator, department, agency who may have received a report or work product affected by the discrepancy.

C. In the case of internal audits, all nonconformities are noted on the Quality / Internal Audit Record form. Any nonconformities noted during audits will be evaluated by the Digital Forensics Lab Manager to determine if a corrective action request is necessary. Upon identification of nonconformity in the quality system, the Digital Forensics Lab Manager will initiate an investigation to identify the root cause and basis of the nonconformity related to a technical procedure. The Digital Forensic Lab Manager shall perform administration and technical reviews on any case where a deviation of policy or procedure took place. The Digital Forensics Lab Manager will also examine the policy or procedure that was deviated from and determine if updates or changes are warranted for that particular policy or procedure. Corrective actions shall be appropriate to the

magnitude and risk of the problem. The Deputy Secretary-IT and Digital Forensics Lab Manager will ensure documentation and implementation of any technical remedies. If necessary, work will be recalled and the customers will be notified about nonconformities.

D. The CAR form will use the following numbering scheme: XX-X, where the first two digits will indicate the year, and the final digit(s) is the next available. The following levels of nonconforming work will be considered in determining a course of corrective action:
   a. A Level 1 nonconformity is a situation or condition which directly affects and has a fundamental impact on the work product of the laboratory and the integrity of the evidence.
   b. A Level 2 nonconformity is one which may affect the quality of the work but does not, to any significant degree, affect the fundamental quality of the work product. The CAR will be issued in a timely manner to minimize the impact of the nonconformity.

E. Where a corrective action is needed, the laboratory shall implement the corrective action most likely to eliminate the problem and prevent recurrence.
   a. Corrective actions can include, but are not limited to, remedial training, issuing a supplemental proficiency test in the discipline or category of testing in which the member had a nonconformity, notifying the contributor(s), issuing supplemental or amended reports, or indefinitely removing the member from casework. A member who has been removed from independent casework because of technical issues will not be reinstated without written authorization from the Digital Forensics Lab Manager or Deputy Secretary-IT. The Digital Forensics Lab Manager will direct appropriate follow-up action to confirm the effectiveness of the corrective action. This may involve review of casework and audits of the digital Forensic Lab. The Digital Forensics Lab Manager will maintain records of nonconformities, quality system complaints and resolutions including the corrective action requests for at least five years.
   b. The Director/ Quality Manager will maintain an open file of all current CARs and not mark as completed until the monitoring requirements of Section E are documented. The Director / Quality Manager will be required to review the Open CAR File monthly and take appropriate actions to complete the CAR cycle. Once a CAR is complete, the hard copy document will be scanned and a digital copy saved in a Completed CAR Folder within the new Document Control & Organization Scheme.

F. Preventative Action

a. Members are encouraged to identify preventive actions as opportunities to improve quality and correct potential sources of noncompliance before they become problems.
b. These opportunities for improvement shall be forwarded through the lab members through e-mail or memorandum. The Deputy Secretary-IT and/or Digital Forensics Lab Manager will evaluate the suggestion. If implemented, they will work with the submitting individual to develop a Preventive Action Request (PAR). As the preventive action is implemented, it shall be monitored for effectiveness as outlined in the PAR. The PAR form will use the following numbering scheme: XX-X, where the first two digits will indicate the year, and the final digit is the next available.

7-0. Document Control

A. The North Carolina Department of Secretary of State Digital Forensic Lab Quality Manual (DFL-QM), administrative procedures, discipline standard operating procedures, work instructions and training manuals are controlled to ensure that they are adequate, approved for use and that only the current versions of the document are in use. These documents are posted on the NC Secretary of State internal website (Intranet – SOSNET). Printed copies of electronically controlled documents used for casework activities must be disposed of within the same work day. Instrumentation manuals or externally produced quality documents are controlled if they provide direction in performing quality-affecting activities unless the manual or documents have been incorporated in their entirety into a discipline standard operating procedure. These documents are maintained either on the NC SOS internal website or within the laboratory.

B. Controlled Document Format

a. Each internally prepared controlled document will bear the following information at a minimum:
   i. the document title,
   ii. the issue date,
   iii. a unique document identifier,
   iv. “Page of ”,
   v. the issuing authority.

b. Each externally prepared controlled document will have a label referencing the master document containing, at a minimum, the following information:
   i. the document title,
   ii. the NC Secretary of State Digital Forensic lab identifier,
   iii. and the issue date and/or revision identification.

C. Controlled Document Approval and Issuance

D. The NC Secretary of State Digital Forensic Lab system’s policy is set forth in the Digital Forensic Lab Quality Manual (DFL-QM). The policy statements have been approved by the Deputy Secretary-IT and the Lab Manager/Quality Manager. The Quality Manager will issue these policies. Any revisions to the Digital Forensic Lab Quality Manual are approved by the Lab Manager.

E. DFL laboratory administrative procedures are found in the DFL Administrative Procedures Manual (DFL-APM). Procedures are used to implement laboratory system policies. These procedures have been approved by the Deputy Secretary-IT and the Quality Manager. The Quality Manager will issue these procedures.

F. Any revisions to these procedures are approved by the Lab/Quality Manager.

G. Laboratory system technical procedures are found in the Digital Forensic Lab Standard Operating Procedures (DFL-SOP). These procedures have been approved by the Deputy Secretary-IT and the Lab/Quality Manager. Approval of the Standard Operating Procedures also includes any instrumentation manuals referred to within the document. The Quality Manager will issue these procedures.

H. Any revisions to these procedures are approved by the Deputy Secretary-IT, and the lab/Quality Manager. Additional technical documentation includes work instructions, training manuals and externally issued national standards. These go through the same approval process as technical procedures.

I. Controlled Document Review
   a. All controlled documents are reviewed prior to approval and issuance for technical and administrative content.
   b. After issuance, each controlled document will be reviewed at least once each calendar year to ensure it reflects current policies, procedures and technology.

J. Controlled Document Maintenance
   a. The Quality Manager or designee will maintain the official internally prepared controlled documents and all archived versions of the same.
   b. The Quality Manager or designee makes all electronic changes to the controlled documents and distributes them for review and approval to the appropriate parties.
   c. Document control approval is handled electronically via e-mail. Electronic document control issuance is handled by the Quality Manager or designee resulting in approved versions being posted on the NC Secretary of State internal website (Intranet – SOSNET).
   d. Any printed copies of electronically controlled documents used for casework activities may not be retained for more than one day. Compliance with this requirement will be documented via quarterly review. All archived versions of internally prepared controlled documents will be marked “Archived” on the front cover or on the CD.

K. Controlled Document Revisions
   a. Any revised or new text of internally prepared controlled documents, along with the date of issue, will be shown in red ink or strike-through with initials and will remain as such until the next revision or annual review of the document. Once revisions are approved, the current document is archived and the new version takes its place on the NC Secretary of State internal website. Revision histories will be updated on the master document list.

L. Standard Operating Procedures
   a. Digital Forensic Lab Standard Operating Procedures will establish uniform requirements and approved analytical procedures for each category of testing.
   b. Work instructions can be created to address equipment operation on an as-needed basis to address differences in equipment or programs.
   c. The Standard Operating Procedures must include at a minimum, if applicable, the following:
      i. Definitions of key terms
      ii. Abbreviations
      iii. Quality control
      iv. Procedures and/or protocols
      v. Performance checking and maintenance of equipment
      vi. Use of controls, traceable reference standards and materials

8-0. Equipment Records/Documentation

A. Records shall be maintained of each item of equipment and its software significant to the tests performed. The records shall include at least the following:

a. the identity of the item of equipment and its software the manufacturer's name, type identification, and serial number or other unique identification
b. checks that equipment complies with the specification the current location, where appropriate
c. the manufacturer's instructions, if available, or reference to their location dates, results and copies of reports of all, adjustments, acceptance criteria, and validation testing
d. the maintenance plan, where appropriate, and maintenance carried out to date
e. any damage, malfunction, modification or repair to the equipment

9-0. Evidence Handling and Case Management

A. Items that are removed from evidence as a result of forensic processing, examining, or comparing, to include but not limited to:

a. computers,
b. laptops,
c. printers,
d. hard drives,
e. floppy disks,
f. CD/DVD's,
g. USB drives,
h. cameras,
i. mobile devices,
j. CD/DVD archives
k. and recovered data for digital evidence

will meet the same requirements for security, integrity, and inventory as the original item. All evidence will be maintained in the appropriate evidence storage area and documented in the Laboratory Information Management System (LIMS).

B. Non-evidentiary photographic prints and other work product or documentation shall be maintained in a manner similar to case file notes or indexed to the case file.

C. The laboratory may discontinue further forensic examinations when a conclusion identifies, includes or eliminates the subject(s) or substantiates the maximum charge to be filed. The Digital Forensics Lab Manager should review both the case file documentation and communicate with the investigator prior to ceasing additional examinations, analyses or comparisons.

D. The Digital Forensics Lab Manager and assigned evidence custodians will determine who has access to the Evidence Room. Those members assigned to the Evidence Room will have primary responsibility for the receipt, storage, transfer, and return of all evidence. All members will be trained to ensure the integrity of evidence is maintained.

E. Digital Evidence

a. Stand-alone hard drives that are submitted for analysis should be placed in protective packaging such as anti-static bags or anti-static bubble packaging.
b. Evidence having the possibility of receiving or transmitting data should be placed in protective packaging such as a clean metal paint can or wrapped in multiple layers of aluminum foil.

c. All computers should be secured in a way that prevents shifting during transport within the laboratory.

F. Evidence Receipt. Evidence must be submitted to the laboratory by either common carrier or hand delivery from the agency or agency representative working the case:

a. Computers must be sealed using evidence tape that will cover all sides of the computer including any drives, power supplies and case openings. If a computer case is found to be "open", it must be put in a cardboard box and sealed with tamper-resistant tape.
b. All external media (CD/DVD's, USB drives, external hard drives, floppy disks, camera media, etc..) may be packaged in a cardboard box or paper bag and sealed with tamper-resistant tape.
c. Any papers, manuals, or pertinent documentation regarding the evidence shall be submitted in a sealed envelope or box.
d. Any laptop computers shall be packaged in a cardboard box and sealed with tamper-resistant tape or taped around the unit using evidence tape.

G. The lab personnel checking evidence into the lab will determine if the evidence is properly sealed. A container is properly sealed if its contents cannot be accessed or powered on in any fashion, if entering the container results in obvious damage/alteration to the container or its seal, and the seal bears the initials or identification of the person sealing the evidence container. The actual seal itself must be sufficient to prevent the possibility of the item(s) contained from being lost or removed without altering the seal or from being contaminated by outside sources so as to alter the integrity of the evidence.

H. If the evidence received is sealed, but does not bear the initials or identification of the person who sealed the evidence container, the lab personnel will place a piece of tamper-resistant tape perpendicularly across the seal with the initials of the person sealing the evidence or reseal the complete package in another container with proper initials and seals. If the evidence is received in an unsealed condition, the lab analyst will inventory the contents, place inventory documentation in the electronic case record and properly seal the container(s).

I. The digital forensic lab staff will:

a. Utilize the LIMS to complete the appropriate information fields.
b. Ensure a completed service request form accompanies each case with each item listed on the form.
c. If evidence is received by common carrier, the evidence records will contain the method of delivery and tracking information.

d. Prepare appropriate case file(s), using the agency case number to track the case in the LIMS.
e. Ensure the case number is visible on the evidence package(s).
f. Initial each container or package across the security tape and onto the package.
g. Ensure evidence will be packaged and sealed in a manner appropriate for the type of evidence except where precluded due to the size or the nature of the evidence.
h. Secure the evidence in the appropriate evidence storage area and document the location in LIMS until transfer to a laboratory member, another laboratory, or return to the submitting agency.
i. Place the case file in the cabinet containing those of cases waiting to be worked.

J. Special storage circumstances. On occasion evidence will arrive that is required to stay plugged in to preserve data integrity (ie: cell phone). In this case, the evidence shall be labeled as required and shall be stored in the evidence room in a manner so that it may be connected to a power outlet. Any other special storage requirements shall be discussed with the Lab Director and determined on a case by case basis.

K. Evidence Marking and Sealing after Initial Intake
a. When a package is opened, the original seal shall be left intact, whenever possible, and a new opening made. When the analysis is complete, the new opening shall be sealed as outlined in these procedures; thus the original package seals will be intact, when possible, and all seals will be clearly marked.
b. A new evidence package may be used upon resealing evidence. The new evidence package shall also be marked and sealed in a manner appropriate for the type of evidence with laboratory seals, documented in LIMS, and marked with the member's initials across the evidence tape onto the package with indelible ink. Wherever possible, the original evidence packaging shall be maintained inside the new evidence packaging.
c. The analyst who inventories the outer package will ensure that the exhibit and/or agency item numbers of the evidence in the package are listed on the outside of the package.
d. In the case of creating a sub-item or new container shall mark the exterior packaging with the item number or the agency exhibit number of the evidence contained within the packaging. Sub-items and new containers will be packaged and sealed as outlined in these procedures.

e. When multiple items or sub-items of evidence are contained within a properly sealed and properly marked container, each item which had its contents analyzed must be marked with the case number, member's initials and either the item number or agency exhibit number. As long as the existence of the remaining items are documented and the outer container is properly resealed, it is not required that the containers holding unexamined items be marked.
f. Evidence which is properly sealed and marked for identification may be placed in unsealed and unmarked containers such as boxes or bags for the purpose of grouping items of evidence or for the convenience of carrying the evidence without that container having to meet the requirements of identification and sealing as long as evidence security requirements are otherwise met.
g. If at any point during evidence handling or analysis a discrepancy is noted on the evidence packaging or paperwork, please refer to the Appendix in this document for appropriate actions. Any deviations from the Appendix requirements must have the documented approval of the Digital Forensics Lab Manager or designee.

L. Evidence Storage and Retention
a. Evidence will be stored in the appropriate evidence storage area until it is transferred to an analyst or returned to the submitting agency.
b. Evidence in the possession of an analyst, but not out for examination purposes, shall be secured in designated evidence areas.
c. If forensic evidence is stored in a location other than the designated evidence room, then the storage facility must meet the same security requirements as outlined in the regional Security and Safety policies and procedures.

M. Evidence Routing and Processing
a. All evidence transfers must be documented electronically in LIMS.
b. In instances where evidence in process must be left unattended in a secure examination area, a notice will be posted signifying the status of the evidence.
c. In the event that a member is not present and evidence must be retrieved from their custody for purposes such as but not limited to court proceedings, the authority will be granted to the Deputy Secretary-IT or designee to administratively transfer the evidence. The administrative transfer will be noted in the electronic case record.

d. If the electronic system is not operational, all transactions will be documented with a manual system and the electronic system updated as soon as feasible.

N. Evidence Return

a. When the analyses are completed, evidence will be transferred back to the evidence room for return to the contributor. These transfers will be recorded as described above. Documentation must be provided to the contributor and electronically maintained.

b. Laboratory personnel will not routinely transport evidence, unless approved by the appropriate Supervisor.

c. Evidence will be returned only to a representative of the original submitting agency, except when released to officers of the court. Evidence may be returned to representatives of other agencies only with direct written authorization from the original submitting agency. A copy of this written authorization shall be maintained (Scanned and added to the case file or attached to the evidence entry in LIMS.). If the laboratory member does not recognize the contributor or recipient, proper identification must be provided with a copy of the identification credential made and added to the case file or evidence entry in LIMS.

d. Evidence may be mailed or shipped. When mailing or shipping evidence the following will apply:

i. Evidence should be routinely sent via U.S. registered mail, return receipt requested, but if necessary, evidence requiring overnight delivery may be sent via common carrier.

ii. Evidence containing contraband must only be mailed via U.S. registered mail, return receipt requested.

iii. When shipping evidence by other than the U.S. Postal Service, the vendor must provide return receipt and be able to track shipment.

O. The Digital Forensics Lab Manager or designee will ensure that submitting agency personnel are notified to pick up completed evidence. If no action is taken by the agency within a reasonable time period, the evidence will, if possible, be returned by the appropriate mail service. Evidence not suitable for mail return will be brought to the attention of the Digital Forensics Lab Manager for resolution.

10-0. Exceptions

A. Due to the very nature of investigations involving technology and the ever changing software, hardware, and analysis equipment there may be times when it is appropriate for a forensic examiner to deviate from written policies or procedures. Certain aspects of an investigation may also dictate the need to deviate from policies and procedures such as exigent circumstances.

B. In rare circumstances it may be necessary for an examiner of the Digital Forensic Lab to deviate from the policies or procedures in place. The deviation may be due to exigent circumstances or incidents where due to an articulated fact, the standard policy or procedure would not allow the examiner to complete a thorough analysis.

C. Documentation Required. In the event that written policies or procedures are deviated from by an examiner, the justification for deviation and the circumstances surrounding the incident shall be documented within the case report. The Digital Forensics Lab Manager shall also be notified.

D. Review of Deviations. The Digital Forensics Lab Manager shall perform administration and technical reviews on any case where a deviation of policy or procedure took place. The Digital Forensics Lab Manager will also examine the policy or procedure that was deviated from and determine if updates or changes are warranted for that particular policy or procedure.

E. Notification of client. In a case where it is necessary to deviate from a standard procedure and the deviation will affect the test results, it must be documented, technically justified, and the client must be notified prior to the deviation for acceptance of the testing.

11-0. Inventories & Inspections

North Carolina Department of Secretary of State Digital Forensic Lab will ensure the quality of operations utilizing periodic inventories and inspections.

A. Evidence Inventory

The Digital Forensics Lab Manager ensure that a complete annual evidence inventory of the laboratory evidence room is conducted.

Additional laboratory evidence inventories may be conducted as determined necessary or desirable by the Deputy Secretary-IT.

B. Property Inventory

The Digital Forensic Lab will annually conduct a complete property inventory of its laboratory.

C. Safety Inspections

The Digital Forensics Lab Manager will conduct a quarterly safety inspection within the laboratory.

D. Chemical & Toxic Substance List
The Regional Safety Coordinator, or designee, will update annually the list of all chemicals and toxic substances in the laboratory and ensure the corresponding Material Safety Data Sheets (MSDS) are available.

12-0. Laboratory Case Record Contents

A. Report writing is an essential part of every examination. An organized, detailed report is critical to the successful prosecution of cases worked by the North Carolina Secretary of State investigators.

B. Report Preparation

a. The Digital Forensic Lab examiner is required to prepare a case report for every case submitted into the lab. All reports shall:

i. be titled “Digital Forensic Laboratory Report”,

ii. shall display the Seal of the NC Department of the Secretary of State on the cover page.

iii. and shall contain the address of the laboratory.

b. Each report shall:

i. contain the case number,

ii. the names and addresses (if known) of the customer

iii. and the names of the parties involved in the case investigation,

iv. all of the findings of the examination,

v. and all actions taken.

vi. All pages shall be numbered

vii. and the case number shall be identified on each page.

c. If data is recorded on both sides of a single page, the examiner must identify and initial each side as a separate page. The examiner shall not distort, conceal or otherwise falsely report any facts regarding the case, either orally or written. Examination records shall be of permanent nature.

C. Report Documentation

a. All of the reported information, whether gathered from the forensic tool that was used for the examination, or included from the evidence management system (LIMS) shall be presented on a document indicating it is from the NC Secretary of State Digital Forensic Lab.

D. If submitted evidence does not require processing at the request of the investigator or submitting representative, the written or typed request must be included in the case file. A case report is not required.

E. The full case report shall contain the following information:

a. Lab number assigned (if different from the case number) on each page

b. Original (submitting agency) case number

c. Name of investigator
d. Suspect name
e. Description of packaging and seals
f. All items submitted as evidence
g. Description and condition of items submitted
h. Received Date
i. Start and End dates of testing
j. Type of examination requested
k. Type of examination performed (method)
l. List of items tested
m. Summary of results
n. Disposition of the evidence
o. Signature and date of the examiner
p. Page number (each side of a page shall be treated as a separate page)
q. Initials of the analyst who prepared the report on each page
r. Name and address of the lab
s. Name and address of the customer
t. Any deviations from or additions to normal test methods
u. Photos of evidence if available
v. Reason for no definitive conclusion if applicable
w. Opinions and interpretations where appropriate
x. Any additional information required by testing methods or customer(s)

F. Summary. When any associations are made as a result of an examination, the significance of the association shall be communicated in the test report. If an individual can be eliminated as a suspect to an investigation as a result of an examination, that elimination must be clearly communicated in the report. If no definitive conclusion can be made, the report shall contain the reason for this. Any opinions and interpretations shall be documented with the basis for the opinion or interpretation.

G. Subcontractor Reports. If an examination is performed by an approved sub-contractor, these results shall be documented and reported by the person performing the exam.

H. Report Access. Any reports generated in the Digital Forensic Lab shall be stored on the lab server or in the case file upon completion of the case. These reports

can only be accessed by authorized personnel and shall not be released or shown to anyone other than lab personnel or the investigator without approval of the Lab Director. All records shall be held secure and in confidence. The lab report shall be released to the case investigator and any person listed on the submittal form by the investigator as a required recipient of the report.

I. Electronic Transmission of Report. Any transmission of a case report via telephone, fax, email or other electronic means shall be documented by the examiner and maintained in the case record.

J. Finalizing and Changes to Reports.
   a. Any changes made to reports shall be crossed out with a single strike, corrected in a legible fashion, and initialed by the author of the change. Nothing will be obliterated or erased. Opaque correction fluid or correction tape shall not be used.
   b. Electronically recorded technical records are considered finalized once the data is submitted for technical case file review. Changes made in electronically recorded technical records after this point must be dated and initialed on the hard copy in the case file. Any changes in electronic form must be:
      i. done by way of a supplemental report,
      ii. shall be identified as a supplemental report,
      iii. and shall not change the original information.
   c. If a supplemental report is necessary for a case that has been previously reported on, the new report must be uniquely identified with the case information and appropriately reference the original report.

K. Reports for Cancelled Requests. At times a case will proceed through the court or be dropped before examinations. Upon notification of the disposition of the case, the examiner shall complete a report documenting the notification date, time, and reason. If there is email or written documentation, this should be included in the case file. The case will then be considered closed and no further action will be performed.

L. Case Record. The full case record folder for a completed case shall:
   a. contain the case report,
   b. any additional reports,
   c. the archived copy of the case in digital format (ie: e.0x files)
   d. and case notes if taken.
   e. If there is any communication regarding the case such as updates via email, they should be included in the case record folder.

f. When the Digital Forensic lab subcontracts work, the Digital Forensics Lab Manager will advise the contributor of the arrangement in writing. The notification will be documented in the lab case record.

M. Lost or Damaged Case File. In the event of a lost, damaged, destroyed, or contaminated case file, a thorough attempt will be made to reconstruct the file folder and its contents. In the case of a damaged or contaminated case file, if possible, the original file should be preserved or photographed. A reconstructed file will be marked as such. This will be done under the supervision of the Digital Forensics Lab Manager with notification to the Deputy Secretary-IT.

N. Case File Retention. Files containing case records shall be maintained in hard copy for 7 years or until cases have been processed through the judicial system, whichever is longer. Case files will be kept in the Digital Forensic Lab evidence room in storage boxes, indexed by case number and separated according to investigative unit (Securities or Trademark). Due to limited storage space, the case will be deleted from the Lab server upon archiving to other appropriate digital media.

O. Administrative Records. All administrative records, either received or generated by the laboratory for a specific case shall be identified with the unique case number used by the laboratory. Each case shall be identified by a unique case number when data is generated on multiple cases on a single printout.

P. Independent Reviews on Critical Findings. If it is necessary to conduct an independent check on a critical finding, the check shall be conducted by an examiner having expertise gained through training and casework experience in digital forensics. A record of the independent review shall contain the reasoning for the review, the name of the examiner performing the independent review and when it was performed.

13-0. LIMS Business Practices

A. A Laboratory Information Management System (LIMS) is a necessary element in keeping track of evidence intake, transfer and release. Chain of custody is a critical point of evidence management, as it helps to ensure the integrity of the evidence has remained intact.

B. Evidence Intake/Transfers
   a. When evidence is received into the laboratory, the Evidence Handling and Case Management Lab Administrative Procedure shall be followed and the evidence must be logged into the Laboratory Information Management System (LIMS).
   b. The current LIMS is located on the Laboratory Storage Server under Evidence Check In_Out.
   c. Select the Evidence Inventory Form for the current year and assign the next available lab number (20##-#) to the case.
   d. Put labels with the lab number assigned to the case on each piece of evidence.

C. The Evidence Inventory Form will include the Agency Case #, the number of pieces of evidence (# of packages), the date received, the agency, and the location of the evidence in the evidence room.

D. Transfers
   a. Upon moving any items of evidence to another shelving unit within the evidence room, the Evidence Inventory Form must be updated with the new location.
   b. Upon transferring any evidence to anywhere outside of the lab, the Evidence Inventory Form must be updated with the Date Returned.

E. Sub Items. Any sub-items that are have been created as a result of general case work shall be updated in the # of Pieces of Evidence in the Evidence Inventory Form.

14-0. Management Continuity

A. When the Deputy Secretary-IT or Digital Forensics Lab Manager will be unavailable to perform their duties, they will designate a member to assume their responsibilities.

B. If the Deputy Secretary-IT is unable to designate an acting director of the entire Digital Forensic Lab in his/her absence, the Digital Forensics Lab Manager will be the acting director of the lab until further notice.

C. If the Digital Forensics Lab Manager is unable to designate and acting manager of the Digital Forensic Lab in his/her absence, the Deputy Secretary-IT will be the acting manager of the lab until further notice.

15-0. Management Reviews

A. An annual management review is required to ensure that laboratory management can continue to be confident that all measures taken provide the highest quality service using "state-of-the-art" technologies. The laboratory will conduct an annual management review to determine if the current quality system is effective.

B. Annual Review. The management review shall be conducted annually and shall be organized by the Lab Manager.

C. Procedure

a. The management review shall include these areas to be reviewed for effectiveness:

i. Suitability of policies and procedures
ii. Reporting from managerial and supervisory personnel
iii. Reports of recent internal audits
iv. Reports of corrective and preventive actions
v. Reports of assessments by external bodies
vi. Results of proficiency tests for examiners
vii. Review any changes in type or volume of cases submitted
viii. Customer feedback
ix. Customer complaints
x. Examiner complaints
xi. Recommendations for improvement
xii. Staff training
xiii. Resource assignment

D. Findings. The findings of the management review should be used to guide the direction for the goals, objectives and plans for the following year. The actions taken to correct, update, or improve Lab efficiency and accuracy shall be organized by the Digital Forensics Lab Manager and done in a timely manner.

E. Record of Management Review. The review and actions taken shall be recorded, along with the actions that are taken as a result of the management review meeting.

F. Management Review Documentation Retention. Documentation of the management review shall be maintained by the Digital Forensics Lab Manager through one cycle of ANAB accreditation or five (5) years, whichever is longer.

G. ANAB Annual Accreditation Review Report

a. The Digital Forensic Laboratory will prepare an annual accreditation review report as required by ANAB.

b. The Digital Forensics Lab Manager will complete the annual accreditation review report for the laboratory. The annual accreditation review report will be completed by the laboratory's accreditation anniversary date of each calendar year.
c. The Digital Forensics Lab Manager will review the reports and forward them to the ANAB Executive Director within thirty (30) calendar days following the laboratory's accreditation date of each calendar year.

H. Accreditation Report Documentation Retention. Annual accreditation review report documentation will be maintained by the Digital Forensics Lab Manager for at least five years.

16-0. Proficiency Testing

A. All laboratory examiners must maintain proficiency in order to ensure quality examinations and to keep up to date on forensic procedures and methodology. The examiner shall complete a proficiency exam once annually.

B. Methods of Testing

C. Lab Director/examiner

a. Digital Forensic examiners shall complete an annual proficiency exam that is given by an outside agency to ensure he/she is maintaining an adequate level of knowledge and providing correct results during examinations of digital evidence.

b. The Lab Director shall maintain the results of the proficiency exams and a copy of the results will be provided to the direct supervisor of the Lab Director to ensure full disclosure.

D. Documentation.

a. Proficiency testing documentation shall include:

i. Identification of test set
ii. How testing was created or obtained
iii. Identity of the person taking the test
iv. Date of analysis and completion
v. Originals or copies of all data and notes supporting the conclusions
vi. Proficiency test results
vii. Any discrepancies noted
viii. An indication that the performance has been reviewed and feedback provided to the analyst
ix. Details of corrective action taken if necessary

E. Remedial Training

a. Lab Director/examiner. In the event any examiner does not pass an external proficiency exam, his or her immediate supervisor will be contacted and the appropriate remedial training will be done.

17-0. Quality and Technical Records

A. Quality Records. The North Carolina Department of Secretary of State Digital Forensic Lab quality records include:
   a. internal and external audits,
   b. evidence,
   c. property inventories,
   d. safety inspections,
   e. management reviews,
   f. annual accreditation audit reports,
   g. quality assurance review forms,
   h. corrective and preventive actions,
   i. training records,
   j. testimony review forms and
   k. proficiency testing documentation.

B. The laboratory is responsible for maintaining and disposing of the quality records; however, the Quality Manager will maintain the official training progress reports and memos, management review, and corrective action records. All records are accessible to the Deputy secretary-IT. The records should be maintained in a file system, whether electronically or hard copy, that is organized for ease of access.

C. All quality records will be maintained for at least five years. Training records will be maintained for the duration of a member's employment with the Digital Forensic Lab. Quality assurance review forms, corrective actions and proficiency test results will be maintained indefinitely. Disposal of quality records should include shredding or electronic deletion.

D. Technical Records. NCSOS DFL technical records include
   a. case records,
   b. validations,
   c. performance checks, and
   d. equipment logs.

E. Completed laboratory case files will contain administrative and technical records and be maintained in secure, designated areas. The case file must also contain information on the location of any examination documentation not present in the case file.

F. Access to case file storage areas will be limited to personnel designated by the Lab Manager.

G. Case File Retention. Laboratory case files will be retained for 10 years or until the case appeals process has completed.

18-0. Resolution of Complaints

A. Complaints lodged against an examiner in the Digital Forensic Lab regarding the work product of the examiner shall be handled according to this policy.

B. All personnel assigned to the Lab have a duty to receive a complaint from anyone wishing to lodge one and forward it to the appropriate supervisor.

C. Complaints about the Lab Manager/Examiner. If a complaint is received about the Digital Forensics Lab Manager it shall be documented and forwarded to the Deputy Secretary – IT.

D. Complaint Investigations. Complaints about the quality of work or discrepancies of forensic findings, improper forensic methodology, unethical behavior, or other issues involving character shall be investigated by the Digital Forensics Lab Manager or Deputy Secretary-IT.

E. Complaints involving a policy violation, inappropriate conduct, unethical behavior, or things of that nature shall be investigated jointly by the Digital Forensics Lab Manager and the Deputy Secretary - IT

F. The Digital Forensics Lab Manager should consult with the Deputy Secretary - IT when necessary concerning these issues.

19-0. Review of Requests

A. Primary Review. Customers have access to the Request for Service form, which is available electronically. Prior to the submission of evidence, laboratory personnel will evaluate the request to ensure that the laboratory has the capability and resources to perform the requested services.

B. The NCSOS Digital Forensic Lab will not routinely conduct reanalysis of evidence that has been previously analyzed by another laboratory unless directed by the court or approved by the Lab Manager.

C. If a request for services is found to be acceptable, this review will be documented by entering the request into the LIMS and preparation of a Case File identifying the examinations to be performed.

D. For hand delivery of evidence, if the request for services is declined, the evidence will not be accepted. For evidence delivered by common carrier, the items will be entered into the LIMS. The reason for the declination will be documented in narrative and a report will be prepared.

E. Secondary Review. After a case has been submitted to the laboratory, but prior to examination (such as at the time of case assignment), the request is reevaluated by the analyst. If the service requested is acceptable, the review will begin, and be documented by assignment of the request to the analyst in LIMS.

F. If it is determined the laboratory is unable to fulfill the service requested, either a report will be issued or the communication with the contributor will be noted in the LIMS narrative. Contact information should include the contributor, date, and time of the communication.

G. In the event that during analysis it is determined that a previously accepted service request is not possible or appropriate, or additional discipline testing is suggested, the appropriate assignment or task will be made or deleted and documentation will be noted in the LIMS narrative. The customer shall be notified of any deviation from the contract.

H. The review shall cover any work that is subcontracted by the Digital Forensic Laboratory.

I. Amendments. Any amendments to the contract that occur after work has commenced require a contract review process and any amendments shall be communicated to the affected personnel.

20-0. Services and Supplies

A. Supply Selection. It is the responsibility of the Digital Forensics Lab Manager to select supplies used within the digital forensic lab. It is the duty of the Lab Director/examiner to provide suggestions on new supplies, vendors, or changes to existing supplies used within the lab. The Lab Director will be asked to provide feedback to the Deputy Secretary - IT on the equipment/software in the lab. Records of these evaluations will be maintained by the Lab Manager. This is applicable only to those materials and supplies that affect the quality of the digital forensic analysis or the validation of equipment in the Digital Forensic Lab.

B. Inspection and Validation. All materials and supplies that affect the test results must be inspected and/or validated prior to being implemented in the laboratory. Record of the compliance or non-compliance will be maintained in the laboratory. Equipment validation will be done according to the Validations and Performance Checks Administrative Procedure.

C. Reporting Faulty Supplies. If the Lab Director/examiner discovers any equipment or software that is not operating correctly or does not meet lab specifications, they should immediately stop using the faulty equipment and document the issue. When the issue is corrected or the equipment is replaces, proper testing measure shall be required to put the equipment back in service. This shall be documented.

D. Supply Purchasing. Notify the Lab Director of any supplies that need to be ordered such as DVD's, CD's and other non-forensic materials. This is to avoid ordering too many supplies. Supplies shall be purchased based on NC SOS purchasing procedures and must meet the requirements of the industry standards. All purchases are approved by the Deputy Secretary-IT.

E. The Deputy-Secretary-IT will initiate the purchase request form upon his/her approval of the purchase. This form will contain a detailed description of the item(s) requested, cost, and vendor information. A check of the supply room will be done prior to ordering.

21-0. Testimony Review

A. Testifying in court is one of the most important functions performed by Digital Forensic Lab personnel. Due to the sophistication and technological content of our testimony, it is critical that members understand the importance placed upon their testimony and forensic findings. The Digital Forensic Lab examiner shall always be truthful and exhibit professionalism while testifying in any legal matter.

B. Testimony. The testimony of a digital examiner is typically unlike the common law enforcement testimony. Occasionally, digital examiners are asked to provide presentations to the court. The use of tools such as PowerPoint and projectors may be required to show the court how particular evidence was located. Examiners should be familiar with these tools and others in order to advise the prosecuting attorney in how their testimony may be given Curriculum Vitae. The Digital Forensic Lab staff is required to keep and maintain a current copy of their curriculum vitae (CV) for courtroom testimony.

C. Attire. Digital Forensic Laboratory staff shall wear business attire when being called to testify as an expert witness.

D. Testimony Evaluation. Courtroom testimony of the digital examiners is evaluated by the Deputy Secretary - IT. A courtroom testimony evaluation form may be sent to officers of the court to evaluate the testimony of the examiner. Evaluation forms will be maintained by the Lab Director for five (5) years or through one cycle of accreditation.

22-0. Training Programs

A. Technology is an ever-changing field and requires constant training to keep updated on the latest technology trends and information. Personnel who perform forensic examinations of digital evidence must maintain a minimum level of training annually.

B. Responsibilities

a. Personnel. The Lab director/examiner is responsible for maintaining a training log that details course titles, dates of attendance, number of hours for the course, course location and whether or not it was tested training. The Lab Director/examiner should notify the Deputy Secretary - IT of upcoming training opportunities for consideration to attend.

b. Lab Director. A master training record will be maintained by the Cyber Crime Lab Director. This will be updated annually. The Lab Director may make recommendations to the Deputy Secretary - IT about upcoming training or areas of suggested training. The training record shall include the management authorization of the employee to perform duties, competence testing, educational and professional qualifications, training and skills and experience of all lab personnel. All forms shall contain the date of which the authorization or competency is confirmed.

c. Digital Forensic Examiners. The field of digital evidence is very challenging and always changing as new software and hardware is developed. It is imperative that individuals assigned to conduct forensic examination be highly trained with an excellent foundation of knowledge in the area of digital media and digital evidence practices. Personnel assigned to the Cyber Crime Lab must meet the minimum qualifications for this position.

C. Digital Forensic Training Program. To maintain a high service level and for the integrity of the Cyber Crime Lab, examiners must complete a rigorous training program prior to conducting independent examinations on any evidence.

a. Training levels:

i. 0-1 years: Digital Forensic Examiner Trainee requires 6 months-1 year of guided lab training

ii. 1-2 years: Digital Examiner

iii. 2+ years: Senior Digital Forensic Examiner has completed all of the training requirements and has obtained necessary certifications.

D. Digital Forensic Disciplines. Depending on the needs of the Cyber Crime Lab and the training and experience of the examiner, new analysts may be assigned to perform certain functions in the lab. The areas of training include:

a. Computer Forensics

Supersedes DFL- APM February 14, 2019
Version 3.1
Destroy Previous Editions
Distribution: All printed copies – Uncontrolled
Document Source: http://sosnet/IT Auth: ACappadonia

b. Mobile Device Forensics

E. Training Manuals. Each discipline above shall have a corresponding training manual associated with it. New examiners must complete the training manual for their position while being assigned to a senior examiner as a lab coach. The Lab Director will meet with the senior examiner assigned and the trainee to review progress regularly. Training manuals will be kept as a part of the employees training file.

F. Training Classes. The Lab Director will recommend outside training to each examiner based on their training and experience. It is highly encouraged that the examiners attend the International Association of Computer Investigative Specialists (IACIS) Certified Forensic Computer Examiner (CFCE) course as soon as possible. Other acceptable training would be SCERS, CCE, NW3C, and some vendor based tool courses.

G. Certification Maintenance. Digital Forensic Examiners shall maintain all digital forensic certifications while employed in the Cyber Crime Lab. In the case of a lapsed certification, written notification by the Lab Director is required. This will be kept in the Lab Directors training file.

H. Minimum Training Hours. The Digital Forensic Examiner must satisfactorily accomplish 20 hours of continuing education in the field of digital forensics. This includes formal classes, online classes and teaching classes related to the field of digital forensics.

I. Completion of Training. Upon successful completion of a Digital Forensic the Lab Director shall maintain the class certificate or a memorandum with the completed class information and hours if a certificate is not available. This will be kept in the examiners training file.

J. Professional Development. The Lab Director/examiner is encouraged to belong to professional organizations related to the Digital Forensic discipline. This is to ensure the examiner is staying current with technology and information. This includes but is not limited to IACIS, HTCIA, and Infragard.

K. Training Library. A library of up-to-date literature and books and a list of available technology-relevant websites and forums will be kept available to the examiner. The examiner is encouraged to read the materials and make others aware of new information they have learned. Articles, guides, whitepapers and other information will be available on the Cyber Crime Lab server.

23-0. Validations and Performance Checks

A. All equipment used by the Digital Forensic lab examiners in the course of examining digital evidence must first be validated to ensure it functions in a manner consistent with product specifications.

B. Required Verifications. The following items must be verified prior to being used in a forensic examination:
   a. Hardware write blocking devices
   b. Forensic imaging software
   c. Forensic examination software
   d. Forensic hardware devices

C. Personnel Conducting Verifications. All forensic verifications must be conducted by personnel assigned to the Digital Forensic Lab, and who conduct forensic examinations of digital evidence or done under their immediate supervision.

D. Verification Reports and Approval. All verifications will be maintained in hard copy in the Lab Forensic Verification Folder within the Digital Forensic Lab. All verifications shall be reviewed by the Digital Forensics Lab Manager and initialed to show they have been approved. Forensic equipment shall not be used in any case until the approval has been given by the Lab Manager.

E. Verification Procedures. Personnel conducting verifications will use the standardized report format created by the Lab. All information about the device or application being tested shall be included in the verification report form, as well as the expected and actual results of the verification. This will be signed and dated by the person performing the validation procedure.

Maintenance Verifications. Hardware verifications need to be done once prior to the equipment being put into service to ensure they function correctly. If any piece of hardware has become damaged, shows obvious wear, or any person in the Lab has questions about its reliability, another validation test shall be performed on the device and documented.

24-0. Appendix

A. No supplemental material.