U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NATIONAL INSTITUTE OF JUSTICE

DIGITAL EVIDENCE

POLICIES AND PROCEDURES MANUAL

May 2020

NIJ.OJP.GOV | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

U.S. Department of Justice
Office of Justice Programs
810 Seventh St. N.W.
Washington, DC 20531

David B. Muhlhausen, Ph.D.
Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
Strengthen Science • Advance Justice
NIJ.ojp.gov

Office of Justice Programs
Building Solutions • Supporting Communities • Advancing Justice
OJP.gov

The National Institute of Justice is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

Contents

INTRODUCTION

Purpose

The purpose of this manual is to give law enforcement agencies a resource that will serve as a starting point for the development of policies and procedures for the collection, handling, and processing of digital evidence.

This manual may also assist agencies performing the accreditation process of the Commission on Accreditation for Law Enforcement Agencies (CALEA) regarding the collection, handling, and processing of digital evidence. This manual is customizable to suit the needs of individual agencies.

Discussion

As society embraces technology and the use of mobile devices increases, a growing number of technological devices are being used in crimes and then seized by law enforcement as evidence. These devices are used by criminals to communicate, store data, and facilitate crimes. Computers, cellphones, GPS devices, digital cameras, and other devices that contain digital evidence must be properly collected, handled, and processed.

The volatile nature of the data on these devices requires proper seizure to preserve the integrity of the data and ensure their evidentiary value in legal proceedings.

Devices must also be processed properly, whether the data they contain are incriminating or exculpatory. It is equally important that these devices are stored in a manner that will preserve the data in their original state for examination by the defense and for the introduction of the original item into court when necessary.

Proper documentation for each device — tracking it from initial submission through storage, processing, the release of any information related to the data on the device, and the return of the device back to the originating agency — will ensure the admissibility of the item and the resulting data in any judicial proceeding.

POLICIES AND PROCEDURES MANUAL

Purpose

Thorough documentation is key to every aspect of criminal justice. Comprehensive policies and procedures are critical components of that documentation. The purpose of this manual is to give law enforcement agencies a starting point for the development of their own policies and procedures addressing the collection, handling, and processing of digital evidence. This document may and should be edited to suit an agency's specific needs in developing its own policies and procedures.

Discussion

Defining a series of policies and procedures can be a daunting task, especially if the author has no experience and no sample policies and procedures upon which to base their drafts. This manual provides a base to work from and build on. The policies and procedures drafted and adopted by an agency should be regarded as a living document and periodically reviewed and updated to remain current and valid. Once a solid foundation for the policies and procedures is established, the process of updating them will become a much more manageable task.

This manual should also assist agencies in complying with the accreditation process of the Commission on Accreditation for Law Enforcement Agencies (CALEA).

Policy

ADMINISTRATIVE STATEMENT

(1) The [YOUR AGENCY]'s Policies and Procedures Manual will contain the current policies, procedures, rules, and guidelines for all laboratory personnel employed and/or assigned to the [YOUR AGENCY] digital forensic lab.

(2) (NOTE: Only if needed) All prior and existing manuals, standard operating procedures, orders, and regulations issued prior to this Policies and Procedures Manual shall be rescinded and replaced.

RESPONSIBILITIES OF PERSONNEL

The contents and revisions of this manual are the responsibility of the lab director or appointed designee. The lab director may issue interim directives as needed, which will remain in effect until such time as they are approved and made a permanent part of this Policies and Procedures Manual. All lab personnel are expected to read and understand the contents of this manual and will be required to sign a document acknowledging they have received a copy of this manual, along with any interim directives, and have read and understood the contents of this manual. The lab director will maintain the original of this document, and a copy will be provided to each individual employed by or assigned to the digital forensic lab.

DISTRIBUTION

Copies of this Policies and Procedures Manual will be distributed to the following:

(1) Lab director

(2) All lab personnel

(3) Lab reference material cabinet or library

This Policies and Procedures Manual will also be available in portable document format (.pdf) on the lab's file server or on another device in a manner accessible by the lab personnel.

CASE ASSIGNMENT AND PRIORITIZATION

Purpose

This section outlines how cases involving digital evidence are received, prioritized, and assigned for forensic analysis.

Discussion

A system must be established to assign cases to lab personnel. Criteria for assignment include priority, case circumstances, examiner skill set, and forensic discipline. This policy will establish the criteria for case assignment and prioritization and the authority to make an exception in case assignment or priority.

Policy

CASE ASSIGNMENT

The lab director or designee will assign all incoming cases. It is possible that a case may be assigned by forensic discipline based on the expertise or current caseload of the examiners or on the needs of the case itself. Unless the submitting agency indicates a need for expedited processing, all cases will be assigned in the order received.

CASE PRIORITIZATION

The lab director or designee will be responsible for identifying cases with a higher priority than others. Priority level will be determined based on the facts known about each case when it is submitted to the digital forensic lab and will be updated as relevant information affecting the priority becomes available.

In collaboration with the investigator, submitting agency, and prosecuting attorney, the lab director will be responsible for identifying cases that may be eligible for early case assessment (ECA). ECA may enable the digital forensic examiners to perform a forensic examination of the submitted digital evidence only to the extent that the prima-facie

case and charges are substantiated, leading to a plea agreement. If a plea agreement is reached as a result of the ECA, no further forensic examination of that digital evidence is required, and the matter may be closed when the case is adjudicated. ECA is very useful for preventing, reducing, or minimizing case backlogs. ECA-eligible cases can be candidates for higher prioritization if they can be cleared more quickly to reduce backlogs and improve the efficiency of justice.

Additionally, cases may be triaged for specific information of investigative value to a case, such as contraband images in a child exploitation case. ECA and triage provide the lab director and staff a way of improving the efficiency of justice and enable examiners to devote more time to more complex cases and cases that contain large volumes of digital evidence.

AN EXAMPLE OF CASE PRIORITIZATION

(1) Terrorism or any case where the loss of life is imminent

(2) Violent crimes such as murder, rape, and assault

(3) A child at immediate risk of exploitation or abuse

(4) Child pornography and solicitation

(5) Theft or destruction of intellectual property

(6) Public corruption

(7) Financial crimes

(8) Internet crimes, including network intrusion and unauthorized access

(9) Identity theft

(10) Fraud

EXCEPTIONS AND MODIFICATIONS TO CASE PRIORITIZATION

All exceptions and/or modifications to case prioritization shall be made by the lab director, or with the approval of the lab director, and include all documentation relevant to the change in case priority.

EQUIPMENT TESTING, VALIDATION, AND UPDATES

Purpose

All equipment and software used by digital forensic lab personnel must first be tested and validated to confirm that it is operating as designed and producing accurate, valid results. Testing and validation must be repeated each time the equipment, firmware, and software are upgraded, reinstalled, or modified. The results of all testing and validation will be recorded and kept on file in order to document that all equipment being used in the collection and processing of digital evidence is functioning within the manufacturer's specifications and the examiner's expectations based on training and experience.

Discussion

In order to determine if hardware or software is working properly, it must be tested by the user and found to perform consistently over time and deliver repeatable results in line with a known dataset each time it is used. This section addresses the need to test and validate each item that is used within the lab and to document the results. Testing steps will be clearly detailed and should be followed in order. It is recommended that as each step in the testing and validation is completed, the person performing the testing and validation should acknowledge completion of the step in writing with initials or another identifiable mark.

Policy

CONDUCTING VALIDATION TESTING

Validation testing will be conducted by all examiners who use any of the collection and processing hardware or software, in any fashion or to any degree, to collect or process digital evidence in the digital forensic lab or at a crime scene.

VALIDATION PROCEDURES

(1) No forensic equipment will be used in the digital forensic lab prior to being tested and validated by lab personnel and approved by the lab director.

(2) Examiners will test each item of hardware and software in a manner consistent with the manufacturer's specifications of usage. Testing will be performed using the same datasets for standardization. All results and anomalies will be documented.

(3) Examiners performing the validation testing on all forensic hardware and software will use a standardized testing and report form, including the date of validation, product name, version number, manufacturer, and cost. All of the validation reports for each item of hardware and software will be approved by the lab director before those items are used in the lab, and all the reports will be maintained on the digital forensic lab server (if available) and also in paper format in a binder maintained within the lab.

(4) All hardware and software will be registered in the lab's name. If the registration must be to an individual, approval from the lab director will be obtained in a memo format, with a copy of the memo maintained on the lab server (if available) and in the lab validation report binder.

MAINTAINING VALIDATIONS

When a piece of equipment becomes damaged or is showing signs of wear or age, it should be tested to verify that it is still operating within the manufacturer's specifications. It is the responsibility of the examiners using the forensic equipment or assigned the item to report such issues to the lab director. The lab director will decide whether to replace faulty, damaged, or worn equipment.

After the initial validation of a piece of software, subsequent validations will be done whenever an update to the software is installed on the lab equipment — including the computers used to examine digital evidence (examination machines) or an item that is considered to be portable. Subsequent hardware validations will be performed each time existing hardware is updated, including firmware updates or installing a new or replacement item, such as a write-blocker. Any hardware upgrades done to an examiner's computer, however minor, should be documented and tested to ensure that they do not affect the performance of the forensic software installed on the computer.

SOFTWARE UPDATES

Updates, patches, or operating system service packs should be installed to the examiner's computer as necessary. The updates, patches, or service packs should be downloaded using a system connected to the internet but isolated from the examination machine and the forensic network. After performing any updates to forensic software, the hard disk drive may be imaged and the image may be maintained for future use in restoring the examiner's computer.

EVIDENCE AND PROPERTY HANDLING

Purpose

The digital forensic lab will receive digital evidence from investigations being conducted by [SUBMITTING AGENCY] and may receive evidence from other law enforcement agencies. This policy will cover the proper handling of all digital evidence and property submitted to the digital forensic lab.

Discussion

In order for devices that contain digital evidence to be properly introduced in any judicial proceeding, the devices must be tracked from the time they enter the custody of the lab through their release to [SUBMITTING AGENCY]. There must be a complete, documented chain of custody from intake to release of each device.

Policy

LAB PERSONNEL RESPONSIBILITIES

The chief responsibilities of all lab personnel when receiving digital evidence or property are maintaining the chain of custody for and ensuring the security of the evidence or property stored in the secure evidence/property room of the digital forensic lab.

RECEIVING DIGITAL EVIDENCE

Only lab personnel on duty at the time the evidence is brought to the digital forensic lab and authorized to receive evidence should accept and document the incoming evidence. When digital evidence is delivered to the digital forensic lab by an investigator or other law enforcement officer, the following steps will be taken:

(1) Lab personnel will ensure all needed documentation is submitted with the evidence. This documentation will include a request for digital forensic lab services and will detail the services requested for each item containing digital evidence.

(2) A copy of the seizure authority, such as a search warrant, consent, or other judicial or administrative order, will be included in the case file. In those matters involving probation or parole, the case file will include a copy of the agreement whereby the defendant waives the right to consent before a search or agrees as a condition of probation or parole to a warrantless search by the Department of Probation and Parole.

(3) Lab intake personnel will list each item of evidence on an inventory document with a number or letter and description, including identifiers and condition. Each evidence item will be marked with the number or letter to readily associate the item with the entry on the inventory document. Subsequent inventories of the evidence will indicate that each entry on the inventory document has been checked and matched to the corresponding evidence item.

(4) The lab intake personnel will sign for the evidence, open a new lab case, and enter the evidence into the evidence tracking system (if the agency has such a system). All items of evidence will then be properly labeled and placed into the lab's secure evidence/property room.

(5) If lab personnel receive additional evidence from a case already opened, they will submit the necessary documentation identified above, along with an updated inventory document. The examiner who is processing the case will be notified that additional evidence has been received.

LABELING

A label will be placed on each item of submitted evidence. The label will contain the case number, originating investigator or agency, lab number, date and time received, and any other information deemed necessary.

HANDLING EVIDENCE IN THE DIGITAL FORENSIC LAB

All evidence contained in the evidence/property room should be sealed properly upon intake and remain sealed until it is removed for examination. The seal should be initialed and dated by the investigator who sealed the evidence. If the evidence is not properly sealed, the individual performing intake for the lab will make a notation on the intake form as to its condition.

a. REMOVING EVIDENCE FROM THE SECURE EVIDENCE/PROPERTY ROOM

When evidence is removed from the evidence/property room, an evidence tracking form will be filled out and kept up to date. Each evidence tracking form will be kept with the case folder. The lab personnel filling out the form will note the date and time, give their name, and provide the reason that the evidence was removed from the evidence/property room. When the evidence is resealed and placed back in the evidence/property room, the date, time, person's name, and location will be updated on the evidence tracking form.

b. EXAMINATION OF SEALED EVIDENCE BAGS OR CONTAINERS

Evidence bags or containers will only be unsealed and opened during inventory or in the course of the digital forensic examination. When unsealing evidence containers or bags,

care should be taken to leave the original seal on the packaging, if possible, and create a new opening in a different location. When the inventory is complete or the examiner is finished with the original evidence, it will be resealed with the examiner's name and initials across the new seal, along with the date and time.

c. EVIDENCE RELEASE PROCEDURE

The lab director will approve all releases of evidence. In the event that evidence is seized by consent and the person to whom the property legally belongs revokes consent, arrangements will be made as soon as possible to return the evidence. Evidence will only be released to the originating agency. In the event that the items being released are forfeited, a copy of the court order declaring the condemnation or awarding the forfeiture will be included in the case file.

d. RELEASE OF EVIDENCE CONTAINING CONTRABAND MATERIAL

Evidence that contains contraband material, such as child pornographic images, will be clearly marked with a label stating "Do Not Release — Contains Contraband." If evidence of this nature will be released to the originating agency, the media will be either:

i. Wiped with an approved wiping method to render the data on the media unrecoverable, or

ii. Accompanied by a form, signed by the case detective and included in the case folder, acknowledging that there is contraband contained in the evidence.

When evidence containing contraband is released to the originating agency, the evidence will be sealed and marked with the date, time, reason for release, name of the lab staff member who released the evidence, and his or her initials over the seal.

e. EVIDENCE DESTRUCTION

The digital forensic lab may from time to time be requested to wipe media, removing all data contained on the media and rendering it unrecoverable. No evidence will be wiped unless a court order is issued or the owner consents in writing. The lab director will first approve all evidence destruction and will maintain a copy of the court order or a signed consent by the owner in the case file. The lab will use an approved wiping method that has been validated and found to render unrecoverable any data contained on the hard drive or other digital media.

f. AUDITS

To maintain the integrity of the evidence/property room in the digital forensic lab, all property contained in the evidence/property room will be inventoried or audited twice a year. Lab personnel designated by the lab director will perform the audit. When the audit is complete, the results will be forwarded in an audit report to the lab director, who will address any anomalies at that time. The audit report will identify each anomaly and its resolution. The lab director will maintain an audit log, along with a list of any anomalies noted or observed.

SEARCH AND SEIZURE

Purpose

This policy provides basic guidelines that may assist lab personnel involved in a search warrant execution. The specific exceptions to the Fourth Amendment's warrant requirement — e.g., plain view,[1] consent,[2] and exigent circumstances[3] — should be handled according to current training and [YOUR STATE OR LOCAL JURISDICTION] law.

Further, the purpose of this policy is to:

a. Process and safeguard digital evidence coming into the custody of the agency.

b. Provide a standardized procedure for the collection and submission of computers and digital evidence for examination and analysis.

c. Document the chain of custody of evidence.

(NOTE: This section is intended as a guide and is not meant to supersede any state or local laws of your jurisdiction. Prior to implementing any information provided in this section, state and local laws regarding search and seizure must be considered. Additionally, information implemented from this section should be approved by your sheriff, chief, or prosecuting attorney.)

Discussion

Everyone is protected from unreasonable searches and seizures under the Fourth Amendment to the U.S. Constitution, and lab personnel will never conduct a search or seize evidence without a valid search warrant or consent of the owner, except when exigent

---

[1] The plain view doctrine is an exception to the Fourth Amendment's warrant requirement that allows an officer to seize evidence and contraband that are found in plain view during a lawful observation.

[2] A warrantless search may be lawful, if a law enforcement officer has asked for and is given consent to search.

[3] Exigent circumstances are those that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts (see United States v. McConney, Ninth Circuit, 728 F.2d 1195).

circumstances exist. This section addresses the general procedures for documenting the execution of a search warrant or seizure by consent as they apply to digital evidence. This section is not intended to address the entire crime scene, but only digital evidence.

(NOTE: This section does not address or encompass all of the circumstances involved in the planning and execution of a search warrant. Different offenders as well as different types of offenses require individualized search warrant execution styles, whether dynamic or passive, and each element of the case should be considered prior to arriving on the scene to execute the search warrant.)

Policy

a. EXECUTION OF SEARCHES

(1) During the execution of a search warrant, all lab personnel will always act in a professional manner, with the safety of all persons being considered first and foremost.

(2) The area containing the digital evidence will be photographed both before and after the search/seizure.

(3) When searching a person believed to have on their person any type of media or devices containing digital evidence — such as mobile phones and USB flash drives — lab personnel or law enforcement of the same sex will conduct the search of that person.

(4) When a search/seizure is concluded, the area searched will be returned to pre-search condition, if possible, and exit photographs will be taken.

b. SEIZING EVIDENCE

(1) Maintaining the chain of custody is a critically important part of any search warrant execution. When seizing evidence, the lab personnel conducting the search and seizure will record where each item was found and its condition at the time of seizure.

(2) When possible, all evidence found will be photographed prior to being moved.

(3) All evidence will be bagged in a proper container, and the bag will contain the case number; the date, time, and location of evidence seizure; a description of the evidence; and the name and initials of the lab staff member or law enforcement officer who found and bagged it.

(4) All evidence will be turned over to the lab staff member assigned as the evidence custodian, or to the person assigned to fill out and maintain the inventory sheet.

(5) A copy of the completed and signed inventory sheet will be left with the owner of the property searched. If the owner is not available, it will be left at the property in accordance with [YOUR STATE OR JURISDICTION] law.

(6) The evidence will be taken to the digital forensic lab, inventoried, logged into the evidence tracking system (if one exists), and labeled according to established procedures.

(7) All evidence will then be secured in the digital forensic lab property/evidence room.

STORAGE AND RETENTION OF EVIDENCE

Purpose

This policy outlines the storage of digital evidence and its retention period in the [YOUR AGENCY] digital forensic lab.

Discussion

There will be times when the digital forensic lab processes devices that contain evidence from the host agency, and there will be times when the digital forensic lab processes devices from outside agencies. This policy is intended to address the need for the storage of all digital evidence, whether from the host agency or from an outside agency.

(NOTE: This section is intended as a guide and is not meant to supersede any state and/or local statutes of your jurisdiction. Prior to using this section, applicable statutes must be considered regarding data retention, and this section should be approved by your sheriff, chief, or prosecuting attorney.)

Policy

a. CREATION OF NEW CASES

When a case is assigned to a forensic examiner and it requires the creation of an image of the digital evidence, a folder will be created on [YOUR AGENCY]'s data storage area/file server, using a uniform naming convention. It is recommended that the assigned case number be used as the name of the folder. Additional folders will be created within the main case folder for the storage of the original evidence image(s). If there is more than one piece of digital evidence to be imaged and examined, there will be subfolders labeled with the evidence number assigned to each.

b. ACCESS TO CASE STORAGE

Forensic examiners and the lab director will be the only lab personnel who have access to the case data storage area. Only the lab director will be able to delete files and folders.

c. EVIDENCE AND RETENTION

All processed evidence from each case will be kept in the case folder created by the examiner during the initial setup for examination. This will include any reports of digital forensic examination, exported files, files generated by the forensic software used, and any other supporting files that belong to the case.

(1) Copies of the reports and supporting files will also be given to the agency or investigator requesting the forensic examination, along with a completed report transfer form.

(2) All submitted items for a particular case — such as computers, hard drives, external hard drives, mobile phones, and USB flash drives — will be released to the investigator at the time he or she receives the report of examination.

(3) The lab director will send an email or letter to the case investigator to get an update on the status of the case. Upon learning the status, the lab director will determine whether to back up the case data, utilizing the means available to the lab at that time (e.g., tape, DVD, Blu-ray disc, hard disk drive, or in compressed format using industry-standard compression software and stored on the file server). A copy of the backup will be kept in a secure area of the digital forensic lab.

(4) A copy of the document releasing the evidence for backup, whether in email format or by letter, will be maintained by the lab director in the case folder.

(5) The lab director or designee will be responsible for removing the case folder from the case file area on the file server (or other storage media) after it has been backed up. The lab director or designee will be responsible for maintaining a record of where the backup is stored.

(6) All output from examination, processed files, and image files will be considered evidence, and the corresponding level of security will be applied and maintained.

(7) In the event that an outside agency has submitted a large number of cases for processing, a single case with a large number of items to be processed, or a number of devices that collectively contain a large amount of data to be processed, that agency may be required to provide the digital forensic lab with its own data storage of sufficient size to back up the case data after it has been processed and removed from the digital forensic lab's file server.

(8) The lab director, on a case-by-case basis, may delete an outside agency's case-related data if the lab's file storage level is critically low and more space is needed for processing ongoing cases.

(9) If an outside agency has not provided any storage device for backing up its submitted evidence:

(a) All efforts to obtain storage media from the outside agency will be made, either by email, letter, or telephone. Copies of the emails or letters will be maintained by the lab director. In the event that telephone calls are made, a report of the calls — including the date and time of each call, the name of the person representing the outside agency, and a summary of the conversation — will be made and maintained by the lab director.

(b) Before the deletion of any case-related data, an additional copy of any narrative-type reports of examination, exported files, files generated by the forensic software used, and any other supporting files that belong to the case will be produced and copied to agreed-upon media.

REPORTS

Purpose

This policy ensures that all lab personnel are aware that a comprehensive final report is a major part of the job of all personnel who examine digital evidence in a case.

Discussion

When a report is well written and organized, it can be interpreted and presented in court so that the judge, jury, and defense will understand the circumstances of the case, the evidence that was found, and how the evidence was found. Additionally, the report should document the acquisition of the forensic image file(s) of the digital evidence, the evidence found to substantiate the charges, and the status or disposition of the digital evidence.

Policy

a. Lab personnel are required to create a report for each case number in [YOUR AGENCY]'s records management system or other case management system. Reports will contain the basic information about the incident, the information requested based on the request for service, all information as to what actions the lab personnel took, as well as their observations, conclusions, and, if necessary, any opinions of the forensic examiners.

b. REPORT DOCUMENTS

The request for service form will contain all of the important information related to the case. At a minimum, it will contain:

(1) Lab case number

(2) Originating agency

(3) Originating agency case number

(4) Name of case agent along with contact information

(5) Suspect name (if known)

(6) Crime and charges

(7) Complete list of evidence submitted and location of evidence

(8) Date and time of evidence intake

(9) What information is being sought (emails, images, etc.)

(10) Short summary of the case and any attachments given by the investigating officer

The final report will include all the above with the addition of:

(1) Examinations conducted (if more than one)

(2) Summary of results and conclusions or opinions

(3) Complete report details

(4) Disposition of evidence

(5) Signature of examiner (digital or handwritten)

c. APPROVAL OF REPORTS

All reports created and edited by lab personnel will be forwarded to the lab director for review and approval. No reports will be released without the approval of the lab director.

d. REVIEWS

All reports submitted to the lab director will go through two reviews, one technical and one administrative.

(1) The technical review will ensure all documents are clearly labeled, all examinations have been conducted, and the examiner's findings are supported by exculpatory or incriminating evidence.

(2) The administrative review will then be performed to ensure any technical issues have been resolved, to find any grammatical errors, and to verify that all the documentation is present and complete.

e. REVIEW DOCUMENTATION

The reviews detailed in section d above will be documented in the review section of the report or on the last page of the report.

f. REPORTS CONTAINING CONTRABAND EVIDENCE

(1) Reports containing images of child exploitation or abuse will be duplicated without the actual contraband images in the report. A copy will be provided to the investigator and the prosecuting attorney's office for providing discovery to the defense.

(2) In the event the investigator or prosecuting attorney requests a copy of the report with the contraband images, a contraband acknowledgment document will be signed by the requesting investigator or prosecuting attorney.

(3) At no time will any reports containing images of child exploitation or abuse leave the digital forensic lab unless there is a court order to supply the images to the defense or a defense expert. The defense attorney or expert will be required to sign a receipt to acknowledge they are in possession of child exploitation or abuse materials and will be required to return the report(s) back to the assigned prosecutor when the case is disposed of.

(NOTE: The rule for discovery regarding the dissemination of contraband images differs from state to state. In this instance, the policy should reflect the rule in the state where it will be in effect. Most states follow the Adam Walsh Child Protection and Safety Act, which limits the defense or defense expert's access to child exploitation material related to the individual charged with a crime or violation.)

g. REPORT STORAGE

All reports in the case folder(s) generated by the examiner and by the digital forensic lab will be saved on the digital forensic lab's servers or accessible storage devices. All handwritten documents or other hard copy documents will be scanned and stored in the case folder on the lab's servers or accessible storage devices.

h. AMENDMENTS TO REPORT

If a mistake or discrepancy is found in a report that has already been issued, that report will be corrected, and an amended copy will be forwarded to the originating investigator or originating agency and to the prosecuting attorney's office as soon as possible. The lab director will be notified immediately, and the report will then be marked "Amended Report."

(1) In the event a report needs an amendment or a supplemental report, it will be submitted to the lab director for review and approval prior to release.

(2) The amended report or supplemental report will then be added to the final report by the lab director.

MATERIALS AND SUPPLIES

Purpose

All materials and supplies used in the digital forensic lab, including consumables, will be approved by the lab director. The content of this policy includes what supplies will be used, who will be responsible for purchasing and maintaining them, and how lab personnel will report deficient or faulty supplies and request additional supplies.

Discussion

In the course of the day-to-day operations of the digital forensic lab, office supplies will be used and expended. These office supplies include, but are not limited to, paper and ink used for printed forms and reports; CDs, DVDs, and Blu-ray discs, if still in use; and file folders and labels.

Policy

a. SUPPLY SELECTION AND PURCHASING

(1) It is the responsibility of the lab director to decide what supplies will be used in the digital forensic lab.

(2) All lab personnel are encouraged to give constructive suggestions as to new supplies, vendors, or changes to the existing supplies used within the digital forensic lab.

(3) All supplies, forensic and nonforensic, will be purchased at the direction of the lab director or with the lab director's approval.

(4) All supply purchasing will be made according to purchasing procedures currently in place at [YOUR AGENCY].

b. REPORTING FAULTY SUPPLIES

Lab personnel who find supplies or equipment that are deficient, faulty, do not perform as expected, or do not meet their intended specifications will notify the lab director by email or memo. Supplies of this nature will be removed from use until the lab director takes action.

c. SUPPLY STOCKING AND INVENTORY CONTROL

Requests for new supplies will be sent to the lab director for approval.

DIGITAL FORENSIC LAB ACCESS

Purpose

The digital forensic lab processes and holds evidence from its own agency and possibly evidence from outside agencies. The evidence that is entrusted to the digital forensic lab contains extremely sensitive data — information or images that are highly confidential in nature. The security of the digital forensic lab and of the data contained therein is essential in maintaining the integrity and chain of custody of the evidence.

Discussion

In order to promote and maintain the highest level of confidence in the examiners, their work product, and their ability to testify in any judicial proceeding, the integrity of the lab as a whole must be guarded at all times. By limiting access to only those individuals who require access, the lab's integrity is maintained at the highest level possible. There will be times when the investigating officer or prosecuting attorney will need to see the evidence in a setting other than a printed report or a report contained on a CD/DVD. In those instances, access will be allowed as long as the individual is escorted by lab personnel and signs a log, which will serve as a permanent record of all the outside individuals who were allowed access to the digital forensic lab. There also may be times when non-law enforcement persons will tour the lab.

Policy

a. LAB PERSONNEL

All personnel assigned to or employed by the digital forensic lab are responsible for the safety and security of the lab. Every effort must be made to maintain the security of the lab at all times and ensure that no unauthorized persons enter the lab at any time.

b. ACCESS TO LAB

(1) All personnel assigned to or employed by the lab will be issued keys and/or credentials for gaining access to the lab.

(2) At no time will any lab personnel share their credentials and/or keys or allow anyone to use them. Violations will result in the possibility of loss of access, assignment to a different division or sector within the agency, or disciplinary action, including but not limited to suspension and/or termination.

(3) If the digital forensic lab is equipped with an alarm system, lab personnel who require 24/7 access will be provided with the code for the alarm system. Whenever the digital forensic lab is unoccupied, the alarm will be activated. (NOTE: In small labs where only one person may be present at any given time, this requirement may be relaxed and the alarm armed only during meal breaks and at the end of the day.)

(4) Access to any area of the digital forensic lab will be limited to authorized personnel only, unless otherwise approved by the lab director.

(5) Law enforcement officers, parole/probation officers, and district attorneys/assistant district attorneys will be granted access to the lab in their official capacity without needing the permission of the lab director, provided each individual signs the entry log and agrees to be escorted at all times.

(6) All non-law enforcement visitors will be required to obtain the permission of the lab director prior to any visit. All visitors will sign in, receive a visitor badge (NOTE: Depending on the size of the lab and agency, this may not be required), and remain escorted at all times. Visitors may be denied access per [YOUR AGENCY]'s visitor policy.

(7) If the lab is equipped with a warning system (such as a flashing blue light) to let all of the personnel in the lab know that non-law enforcement visitors are in the lab, this system will be activated prior to the entry of any non-law enforcement visitors. When the system is active, all examiners will minimize all programs on their monitor screens to prevent the visitors from observing any case-related data.

(8) Defense attorneys and defense experts will not be allowed access to the lab under any circumstances.

(NOTE: If possible, a viewing room or other suitable setting will be provided for defense attorneys and defense experts to access the evidence related to their clients. The lab should obtain an agreement or court order that prohibits the defense from copying any contraband data. The agreement or court order should also allow lab personnel to examine for contraband material any hard disk drive or other media used by the defense during the evidence viewing.)

(9) Maintenance and cleaning personnel will not enter the digital forensic lab unless escorted by lab personnel and will be required to sign the visitor's log.

RELEASE OF INFORMATION TO THE MEDIA

Purpose

This policy regulates and provides guidance regarding the release of information to the news media and media access to the digital forensic lab.

Discussion

When a crime has been committed, the community looks toward the police department or the sheriff's office for information. There must be a sole point for the release of information on cases that impact the community as a whole. However, the digital forensic lab facilitates the processing of evidence and thus cannot be responsible for the release of information to the media.

Policy

a. RELEASE OF INFORMATION

The release of any information to the media, or otherwise granting access to the digital forensic lab, will be the sole responsibility of the lab director — or in those instances where appropriate, of a superior officer, such as the chief of police or the sheriff. In the lab director's absence, the responsibility for determining the media's access to the lab will lie with whomever the lab director designates.

b. REQUESTS BY NEWS MEDIA

(1) Any request for information received by the lab from the media will be forwarded to the lab director, who will refer the inquiry to the agency in charge of the case in question. In the event that this agency is the host agency of the digital forensic lab, the request will be directed to the agency's public information officer or to the officer designated to release information to the media.

(2) Any other requests by the news media for information regarding any current investigations, or for access to the digital forensic lab, will be referred to the lab director or superior officer, unless prior authorization has been given to a specific lab employee for the release of information.

(3) In cases that involve multiple law enforcement agencies, news releases will be coordinated with each of the agencies involved. If possible, each agency will have a representative present during any news releases.

QUALITY ASSURANCE POLICY AND PROCESS

Purpose

Quality assurance ensures that the digital forensic lab is meeting the needs and expectations of [YOUR AGENCY], as well as the needs and expectations of any outside agency that submits digital evidence to the lab.

Quality assurance refers to the planned and systematic activities implemented to ensure that the quality requirements identified for and expected of a product or service are met. It encompasses evaluation, measurement, comparison with standards, monitoring of processes, and feedback that identifies the existence or absence of errors in the results.

Discussion

The digital forensic lab has an ongoing quality assurance program that is designed to monitor the quality of the examination process and provide for continual assessment of and improvements on this process. Quality assurance applies both to the hardware and software employed in the lab and to the work products from each lab examiner. Lab staff will identify and rectify any problems that may affect the lab's performance, the investigative process, or the prosecution of offenders.

Policy

a. OBJECTIVE

The purpose of this quality assurance policy is to:

(1) Build, maintain, support, and document an ongoing quality assurance program that includes effective and organized processes for monitoring, collecting, and evaluating all critical information about important aspects of lab performance in order to identify those areas that have identifiable room for improvement.

(2) Assist in the improvement of each examiner's work processes and work products by focusing on identifying (through the use of continuous evaluations), correcting, and following up on any issues or problems that affect the overall performance of the digital forensic lab.

(3) Implement corrective action when problems or improvement opportunities are identified.

(4) Follow up on identified problems to ensure improvements have been made or corrective actions taken and to ensure a timely resolution with complete documentation of the corrective actions or improvements.

b. INDICATORS OF QUALITY ASSURANCE

Indicators of quality assurance are actively evaluated to maintain an established standard of lab performance. Data from each indicator area will be collected, recorded, and analyzed. The findings will be evaluated to detect any deficiencies and any areas of the process that could be improved upon. When required, appropriate corrective action will be implemented and documented.

Post-corrective monitoring will ensure that the action taken was appropriate and resulted in the proper resolution of any problems or issues found.

(1) PROFICIENCY TESTING

(a) Proficiency programs are designed to ensure that examiners are proficient and efficient. The lab will participate in external proficiency examinations, such as the International Association of Computer Investigative Specialists' certification and recertification programs, as well as the lab's own internal proficiency examinations.

(b) The lab supervisor or designee will review the final results of all proficiency testing and discuss those results with the employee.

(c) A copy of every external proficiency test taken by each employee will be kept in the External Proficiency Testing file.

(d) A copy of every internal proficiency test taken by each employee will be kept in the Internal Proficiency Testing file.

(e) If there are any noted deficiencies in either the internal or external proficiency examinations, those deficiencies will be investigated by the lab manager. A deficiency report will be created, and the lab director will include an explanation of the likely cause(s) of the deficiency along with appropriate corrective action that will be taken.

(2) COMPLAINTS

Complaints received by the lab are monitored for response, corrective action, and follow-up. The lab director or designee will respond to any written or oral complaint deemed significant that concerns the lab's quality of service or work product. The timeline for responding to complaints will follow [YOUR

AGENCY]'s policy. Responses to complaints will be maintained by the lab director for review and any additional recommendations of appropriate action.

(3) TRAINING FOR NEW EMPLOYEES

Lab-specific job descriptions detailing the duties of each employee will be kept on hand in the individual personnel files. Each employee will read, understand, and sign an acknowledgment of their particular job description. In addition to these job duties, a checklist for the training of new personnel will be established for each of the assays performed in the lab. Personnel in training, as well as the staff conducting the training, will sign each section on the checklist as it is completed. These records will be kept in the personnel file and will be available for inspection.

(4) NEW PROCEDURES AND NEW EQUIPMENT

Each employee will be trained on new procedures and new equipment. The training will be documented and signed by the employee and the trainer. These records will be kept in the employee's personnel file and will be available for inspection.

(5) CONTINUING EDUCATION AND TRAINING

Continuing education provides personnel an opportunity to review and expand their knowledge of the digital forensic lab and its processes, facilitating successful lab operations. Each lab examiner is required to complete a minimum of 10 hours of continuing education per year through training conferences, seminars, workshops, and vendor-specific training. It is strongly suggested that each employee keep a record of his or her continuing education.

c. MANAGEMENT REVIEW

The objectives of management review are:

(1) To establish that the quality assurance program is achieving the expected results, meeting the digital forensic lab's requirements, continuing to meet customers' needs and expectations, and functioning in accordance with the established policies and procedures.

(2) To expose deficiencies or defects in the workflow of the lab, identify weaknesses, and evaluate possible improvements.

(3) To review the effectiveness of previous corrective actions, and to ensure that the established quality assurance program is meeting the current needs of the lab and will meet the lab's needs in the future.

(4) To review any complaints received, identify the cause, and recommend corrective action if required.

(5) To review the findings of internal and external audits and identify any area(s) for possible improvements.