**YOUR LOGO HERE**

**Administrative Policy Manual /**

**Quality Assurance Manual**

**DOCUMENT CONTROL #**

**CLASSIFICATION LEVEL HERE**

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) exemption number and category: **7, Law Enforcement**

**Department of Name of Agency review required before public release**

Name/Org: Your name/org Date:

Guidance (if applicable):

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Pages Affected | Description | Author/Editor |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Chapter 1 – Organization and Administration 5](#_Toc403602859)

[Policy 100 – Policy Manual 6](#_Toc403602860)

[Policy 101 – Interim Directives 8](#_Toc403602861)

[Policy 102 – Organization and Structure 9](#_Toc403602862)

[Policy 103 – Training Development Policy 10](#_Toc403602863)

[Policy 104 – Courtroom Testimony 15](#_Toc403602864)

[Policy 105 – Case Triage, Assignment, and Prioritization 17](#_Toc403602865)

[Policy 106 – Control of Materials and Supplies 20](#_Toc403602866)

[Chapter 2 – Property and Evidence Control 22](#_Toc403602867)

[Policy 201 – Property and Evidence Control 23](#_Toc403602868)

[Policy 202 – Evidence Retention and Destruction 28](#_Toc403602869)

[Policy 203 – Physical Access 30](#_Toc403602870)

[Policy 204 – Fire and Evacuation Plan 32](#_Toc403602871)

[Policy 205 – Facility Safety and Maintenance 33](#_Toc403602872)

[Policy 206 – Health and Safety Program 35](#_Toc403602873)

[Chapter 3 – General Operations 37](#_Toc403602874)

[Policy 301 – News Media Relations 38](#_Toc403602875)

[Policy 302 – Report Writing 40](#_Toc403602876)

[Policy 303 – Equipment Testing and Verification 45](#_Toc403602877)

[Policy 304 – Master Case File Documentation 47](#_Toc403602878)

[Policy 305 – Storage of Digital Evidence and Forensic Images 49](#_Toc403602879)

[Policy 306 – Release of Information 51](#_Toc403602880)

[Policy 307 – Deviation from Policies and Procedures 52](#_Toc403602881)

[Chapter 4 – Personnel 53](#_Toc403602882)

[Policy 401 – Proficiency Testing 54](#_Toc403602883)

[Policy 402 – Personnel Records 56](#_Toc403602884)

[Policy 403 – Clothing and Attire 57](#_Toc403602885)

[Policy 404 – Complaints Regarding the Quality System 59](#_Toc403602886)

[Policy 405 – Personnel Complaints 60](#_Toc403602887)

[Policy 406 – Corrective Action 61](#_Toc403602888)

# Chapter 1 – Organization and Administration

|  |
| --- |
| Policy 100 – Policy Manual |

**100.1 PURPOSE AND SCOPE**

The Administrative Procedure Manual for the [Agency Name] is hereby established and shall be referred to as the, “Administrative Policy Manual” and “Quality Assurance Manual”. The Administrative Policy Manual/Quality Assurance Manual is a statement of current policies, procedures, rules, and guidelines for personnel operating within the laboratory. All personnel are to conform to the provisions of this manual. All prior and existing manuals, orders, and regulations, which are in conflict with this manual, are revoked.

**100.2 RESPONSIBILITIES**

The ultimate responsibility for the contents of the manual rests with the laboratory director. The laboratory directory shall be considered the ultimate authority for the previsions of this manual. The laboratory director may issue interim directives, which shall remain in effect until such time as they are permanently incorporated into this manual.

100.2.1 Quality Assurance Review

The review and amendment of this manual is the responsibility of the laboratory director. Laboratory staff may propose amendments of the quality assurance manual at any time. A formal review of this manual will occur annually.

**100.3 OTHER PERSONNEL**

All personnel who have a suggestion to revise the contents of the Administrative Procedure Manual shall forward their suggestion, in writing, to the lab director who will consider the recommendation.

**100.4 DEFINITIONS**

The following words and terms shall have these assigned meanings, unless it is apparent from the content that they have a different meaning:

**Laboratory Director** – The Laboratory “Lab” Director is the person responsible for supervisor, leadership, and management of the laboratory.

**Quality Manager** – The Lab Director shall serve as the Quality Manager.

**Safety Manger** – The Individual response for the health and safety program.

**Shall** – Indicates a mandatory action.

**Should (or may)** – Indicates a permissive or discretionary action

**100.5 DISTRIBUTION OF MANUAL**

Copies of this manual shall be distributed to the following:

* Lab Director
* All lab personnel
* Lab reference manual cabinet

This manual will also be available in digital format on the lab server.

**100.6 MANUAL ACCEPTANCE**

As a condition of being assigned to the laboratory all personnel are required to read and obtain necessary clarification of these policies. Personnel are required to sign a statement of receipt acknowledging that they have received a copy of this manual and understand that they are responsible to read and become familiar with its contents.

**100.7 REVISIONS TO POLICIES**

All personnel are responsible for keeping informed about revisions to this manual. All revisions to this manual will be provided to personnel who must read the revisions and sign the policy manual revision form indicating they received an updated copy.

|  |
| --- |
| Policy 101 – Interim Directives |

**101.1 PURPOSE AND SCOPE**

Interim directives may be issued by the lab director to make immediate changes to policy and procedure. Once issued, interim directives supersede any existing policy or procedure of this manual.

**101.2 INTERIM DIRECTIVE PROCEDURE**

Interim directives shall be issued in writing by the lab director and will be given to all personnel within the laboratory. Interim directives will be numbered with the year followed by the number for that calendar year. For example, the first interim directive for the year 2015 would be numbered, “Interim Directive 2015-01”.

Once the interim directive has been incorporated into the manual it shall be rescinded.

**101.3 RESPONSIBILITIES**

101.3.1 Laboratory Staff

All personnel assigned to the laboratory shall review interim directives and sign a form acknowledging the receipt of the form. All personnel are expected to understand the interim directive or obtain the needed clarification.

101.3.2 Lab Director

The lab director shall issue all interim directives.

|  |
| --- |
| Policy 102 – Organization and Structure |

**102.1 PURPOSE AND SCOPE**

The organizational chart for the laboratory is shown below:

**INSERT ORGANIZATIONAL CHART HERE**

|  |
| --- |
| Policy 103 – Training Development Policy |

**103.1 PURPOSE AND SCOPE**

Technology is an ever-changing field and requires constant training to keep abreast of the latest trends and information. Personnel who are involved either the forensic examination of digital evidence or high-tech crime investigation must maintain a minimum level of training annually.

**103.2 RESPONSIBILITIES**

103.2.1 PERSONNEL

Each laboratory member is responsible for maintaining a training log, which indicates course titles, dates of attendance, hours of course, course location, and whether or not it was tested training. Personnel should also bring upcoming training opportunities up to the lab director for consideration to attend the training.

103.2.2 LAB DIRECTOR

A master training record will be maintained by the lab director for each member, which will be updated annually. The lab director may make recommendations to personnel about upcoming training or areas of deficiencies. The lab director may also provide in-house training to personnel in areas he/she feels necessary.

**103.3 PERSONNEL CONDUCTING FORENSIC EXAMINATIONS**

Digital evidence forensics is extremely demanding and always changing as new software and hardware is developed. It is imperative that individuals assigned to conduct forensic examinations be highly trained with an excellent foundation of knowledge in the area of information technology and digital evidence practices. Personnel assigned to the laboratory for digital evidence forensics must meet the minimum qualifications for this position. Agencies assigning personnel must also sign the Memorandum of Agreement. Personnel assigned to the laboratory for the purposes of digital forensics may be sworn or non-sworn law enforcement personnel.

To maintain a high service level and for the integrity of our laboratory individuals must complete a rigorous training program prior to conducting independent examinations on any evidence.

The training levels are as follows:

* 0-1 years: Forensic Examiner Trainee – Approximately six months to 1 year of training
* 1-2 years: Forensic Examiner
* 2+ years: Senior Forensic Examiner – Has completed all training manuals and

necessary certifications.

**103.4 TRAINING PROGRAM - FORENSICS**

New members of the laboratory who are assigned to the forensic examination of computers or video evidence must complete the training program. Forensic Examiner Trainee’s will be assigned to a coach who is a Senior Forensic Examiner and qualified in each sub discipline they are evaluating the new employee in.

Trainees are not to conduct independent forensic examinations of digital evidence at any time until and unless they have been moved to a Forensic Examiner status. Typically the initial training takes six months to complete, however the lab director upon consultation with the trainee’s coach may make exceptions.

103.4.1 DISCIPLINES

Depending on the needs of the laboratory and the background of the analyst new members may be assigned to different areas of the lab. The potential areas of training include:

* Computer Forensics
* Mobile Device Forensics
* Video Forensics

103.4.2 TRAINING MANUALS

Each discipline listed above has a corresponding training manual associated with it. New members must complete the training manuals for their assignment while assigned to a coach. The lab director will meet on a regular basis with the coach of a new employee to review progress. Completed training manuals will be kept indefinitely by the lab director within the training file of the employee.

103.4.3 OUTSIDE TRAINING

The lab director will recommend outside training to each forensic examiner based upon their training and experience. It is highly encouraged that forensic examiners attend the International Association of Computer Investigative Specialists (IACIS) Certified Forensic Computer Examiner course as early as possible.

103.4.4 IN-HOUSE TRAINING

The lab director is responsible for providing, at a minimum quarterly training for all personnel assigned to the laboratory. This training will include various topics such as policy updates, new technologies, new lab equipment, new procedures, and various forensic topics. The lab director may also have other members present topics as part of their duties. This training will be applied to the minimum number of training hours for employees.

Examiners are also encouraged to maintain memberships to digital forensics list serves, and read applicable journals and publications in addition to in-house and outside training.

103.4.5 CERTIFICATION MAINTENANCE

Members may be required to maintain all digital evidence certifications while assigned to the laboratory. Members must receive written permission from the lab director before allowing a certification to lapse.

Lab members who are sworn law enforcement officers must also comply with the requirements to maintain Police Officer certification.

103.4.6 MINIMUM TRAINING HOURS

Each person who is assigned to forensic examinations of digital evidence must attend at least

20 hours of classroom time in computer forensics or relative investigations annually.

103.4.7 COMPLETION OF TRAINING

Once a forensic examiner successfully completes their initial training the lab director shall meet with the trainee and discuss their training period. The lab director will discuss other training opportunities, areas to improve upon, and solicit feedback about the training program from the trainee. Information about the trainee’s future interests and training desires will also be discussed. The lab director will issue a memorandum to the trainee, all members of the laboratory and the agencies who assign personnel to the lab indicating the successful completion of the employee’s training program.

**103.5 COMPETENCY TESTING**

Prior to any actual case work being handled solely by the new examiner, the examiner shall be competency tested in the disciplines and sub-disciplines they will be functioning in.

**103.6 TRAINING PROGRAM – SUPPORT STAFF/EVIDENCE TECHNICIAN**

Support staff working within the laboratory must be trained in handling digital evidence as well as property and evidence laws, rules and regulations. Support staff that is working with digital evidence must complete the evidence training manual.

103.6.1 IN-HOUSE TRAINING

Support staff may be trained by members of the laboratory in areas such as how to recognize digital evidence, proper handling and storage of digital evidence and how to transport digital evidence. Training may also include how to complete necessary paperwork for chain-of- custody, working on-scene during search warrants or other large incidents, and courtroom testimony.

103.6.2 OUTSIDE TRAINING

Support staff should attend additional training in the area of property and evidence control, liability issues surrounding evidence retention and preservation, and current topics affecting the support staff duties.

**103.7 PROFESSIONAL DEVELOPMENT**

All members of the laboratory are encouraged (and sometimes required) to belong to professional organizations that are associated with their job.

The lab director will present materials to employees at various times to discuss latest trends, new case law or general topics of interest to ensure that laboratory members are staying current with technology and information. Forensic examiners should be part of the IACIS list serve and are encouraged to belong to several other forensic list serves including but not limited to:

* High-Tech Crimes Consortium (HTCC)
* Forensic Video Analysis (VFA)
* Cell phone Forensic List Serves (such as MFI)
* Apple Computer Forensics List Serve

Members assigned to this laboratory will get a wide variety of in-house training and outside training annually as described in this policy. If a laboratory member feels they need additional training or have a particular interest they should advise the lab director.

103.7.1 TRAINING LIBRARY

The laboratory maintains a library of up-to-date literature and books available to all personnel. They are encouraged to read the materials and make others aware of new information they have learned. In addition to books, dozens of articles, guides, whitepapers, and other information documents are available on the lab server.

|  |
| --- |
| Policy 104 – Courtroom Testimony |

**104.1 PURPOSE AND SCOPE**

Testifying in court is one of the most important functions performed by laboratory members. 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. Laboratory members shall always be truthful and exhibit professionalism while testifying in any legal matter.

**104.2 PRESENTATIONS**

The testimony of a laboratory member is typically unlike the common law enforcement testimony. Often laboratory members are asked to provide presentations to the court, which may include the use of PowerPoint and projectors to show the court how particular evidence was located.

Laboratory members should be familiar with PowerPoint and the laboratory projector and practice all courtroom presentations before trial, preferably with the prosecuting attorney present.

It is possible that any computers used to present evidence in trial may be required to stay with the jury during deliberations. Laboratory members should be aware of this fact and ensure that the laptop computer used has no confidential information or evidence for other matters that a jury member or officer of the court may see.

**104.3 CURRICULUM VITAE**

All laboratory members are required to keep and maintain a current curriculum vitae (CV) for courtroom testimony. The lab director shall also maintain a copy of the current CV in the training file of each member.

**104.4 ATTIRE**

104.4.1 GRAND JURY

Laboratory members who are called to testify in front of a Grand Jury shall wear business casual attire at a minimum. Suggested clothing would include slacks with a dress shirt, however a shirt and tie is also acceptable. Support personnel called to testify shall wear their normal daily uniform.

104.4.2 TRIALS AND HEARINGS

* Forensic Examiners – If testifying in front of a jury or if testifying as an expert witness in digital evidence forensic examiners shall wear a suit and tie. If testifying in a bench trial or a hearing (such as a deposition) without a jury a shirt and tie is the minimum requirement.
* Support Staff – Shall wear their normal uniform at any court appearance or hearing.

**104.5 TESTIMONY EVALUATION**

Courtroom testimony of laboratory members is evaluated by the lab director. The lab director may attend court cases and watch forensic examiners testify and/or a *Courtroom Testimony Evaluation Form* may be sent to officers of the court to evaluate the testimony of the member. Evaluation forms will be maintained by the lab director in the member’s file.

|  |
| --- |
| Policy 105 – Case Triage, Assignment, and Prioritization |

**105.1 PURPOSE AND SCOPE**

The laboratory investigates hundreds of criminal cases each year. This policy discusses how those cases are received, triaged, prioritized, and assigned for forensic analysis. This policy applies to all members of the laboratory.

**105.2 CASE PRIORITIZATION**

Once a case is accepted into the laboratory the lab director is responsible for prioritizing cases. Cases submitted by participating agencies will be worked first, then contributing agencies, and finally user agencies. Cases will be further prioritized within their individual agency classifications.

105.2.1 CASE PRIORITIZATION WITHIN AGENCY CLASSIFICATION

Cases shall be further prioritized within each agency classification. Generally the lab director will prioritize cases based upon the facts known to him/her at the time of prioritization. Cases will be prioritized as set forth below for processing and examination:

1. Matters involving or affecting national security;
2. Imminent credible threat of serious bodily injury or death to persons known or unknown, including examinations of evidence necessary to further the investigation of an at-large or unknown suspect who poses an imminent threat of serious bodily injury or death to persons known or unknown;
3. Potential threat of serious bodily injury or death to person(s);
4. Imminent credible risk of loss of or destruction to property of significant value;
5. Immediate pending court date, or non-extendable, outcome-determinative legal deadline;
6. Potential risk of loss of or destruction to property, or exam needed to further the investigation; and
7. No credible potential threat of bodily injury or death to person(s) and/or loss or destruction of property.

105.2.3 CASE PRIORITIZATION SPECIFICALLY FOR ICAC RELATED CASES

In cases that are exclusively Internet Crimes Against Children (ICAC) cases, the following prioritization scale shall be used:

1. A child is at immediate risk of victimization
2. A child is vulnerable to victimization by a known offender
3. A known suspect is aggressively soliciting a child(ren)
4. Manufacturers, distributors or possessors of images that appear to be home photography with domiciled children
5. Aggressive, high-volume child pornography manufacturers or distributors who either are commercial distributors, repeat offenders, or specialize in sadistic images
6. Manufacturers, distributors and solicitors involved in high-volume trafficking or

belonging to an organized child pornography ring that operates as a criminal conspiracy

1. Distributors, solicitors and possessors of images of child pornography
2. Any other form of child victimization.

105.2.4 EXCEPTIONS AND MODIFICATIONS TO CASE PRIORITIZATION

Under special circumstances and on a case-by-case basis the lab director may authorize a case to be investigated outside of its normal prioritization classification. For example, if a user agency submits digital evidence in a homicide investigation and they believe the evidence may lead to the identification of the suspect, the full resources of the laboratory may be assigned to that case, ahead of participating and contributing agency cases for the good of society.

This reassignment will only be for the duration of the exigent circumstance. Once the agency’s need passes any additional evidence in that investigation will be processed at the normal priority level.

**105.3 ASSIGNMENT OF CASES**

Generally, cases shall be assigned to laboratory members at the discretion of the director without regard of the submitting agency, except that specific cases or categories of cases requiring specific security clearance or lawful authority (e.g., secret state or federal grand jury investigations requiring expressed court authorized disclosure, Foreign Intelligence Surveillance Act (FISA) or other national security matters) may be specifically assigned by the director based upon such other criteria.

Cases will, in general, be assigned on the basis of case priority, as set forth herein, and the experience and workload of a member.

|  |
| --- |
| Policy 106 – Control of Materials and Supplies |

**106.1 PURPOSE AND SCOPE**

Materials used in the forensic examination of digital evidence should be standardized and approved by the lab director. This policy discusses supplies to be used, who is responsible for maintaining supplies and how to report faulty equipment. This policy only applies to supplies that actually affect the quality of forensic analysis or the calibration checks of equipment.

**106.2 SUPPLY SELECTION**

It is ultimately the responsibility of the lab director to select supplies used within the forensics lab. All personnel within the lab are encouraged to provide suggestions on new supplies, vendors or changes to existing supplies used within the lab. Laboratory personnel will also be asked to provide feedback and input on supplies used within the lab.

**106.3 REPORTING FAULTY SUPPLIES**

Laboratory members who discover supplies that are not functioning as they should, or do not meet lab specifications should immediately notify the lab director in person or via e-mail. All personnel have the duty and authority to immediately stop using faulty equipment and supplies whether or not the lab director is available.

**106.4 SUPPLY PURCHASING**

Non-forensic supplies such as CD’s, DVD’s, toner cartridges, etc. will be purchased by the Support Specialist with the direction of the lab director. All forensic equipment such as computers, write blocking devices, and software will be purchased by the lab director.

Supplies shall be purchased based upon purchasing procedures in place by the laboratory. Supplies must meet the requirements of the laboratory and industry standards.

106.4.1 SUPPLY STOCKING / INVENTORY

Non-forensic supplies will be stocked and inventoried by the Support Specialist. The Support Specialist shall ensure that supplies are always available and order new supplies when needed.

106.4.2 ACCEPTABLE SUPPLIES

The following have already been tested and approved for use within the laboratory:

* Maxell CD’s and DVD’s
* Memorex CD’s and DVD’s
* HP CD’s and DVD’s
* All HP Printing supplies

For forensic equipment, refer to the verification manual.

**106.5 SUPPLY TESTING**

Forensic supplies (write blockers, software, etc.) shall be tested and verified prior to being placed in service and being used for an actual case. For a forensic computer this may be as simple as booting the computer and ensuring that all internal components work properly and the computer functions normally. For forensic write blocking devices and forensic software, a full verification or validation shall be done (refer to laboratory verification manual for further information).

Forensic supplies will be tested directly by, or under the immediate supervision of a forensic examiner.

**106.6 INVENTORY OF SUPPLIES**

All forensic software and hardware used within the laboratory will be inventoried and documented annually to ensure it is in working order and in the proper location and accounted for.

# Chapter 2 – Property and Evidence Control

|  |
| --- |
| Policy 201 – Property and Evidence Control |

**201.1 PURPOSE AND SCOPE**

The laboratory receives digital evidence from a variety of local, county, state, and federal law enforcement agencies. This policy covers the procedures for all aspects of evidence handling.

**201.2 PERSONNEL RESPONSIBILITIES**

Chain of custody and the protection of evidence are paramount to our operations. All personnel have the responsibility of protecting evidence stored in the laboratory.

**201.3 RECEIPT OF DIGITAL EVIDENCE**

Evidence will be received from any Participating and Contributing Agencies at all times. Evidence may be accepted by User Agencies on a case-by-case basis. The lab director or the Support Specialist may, upon their discretion, deny a case submitted by a User Agency in certain circumstances. These circumstances may include, but are not limited to; Lack of legal authority to conduct investigation/analysis, uncooperative case agent, condition of evidence submitted, and type of case (e.g., minor violations or misdemeanors). Cases such as homicide investigations, missing children, or endangered missing adults will be investigated for any law enforcement agency regardless of their status.

When a law enforcement officer delivers digital evidence to the laboratory the following steps shall be taken:

1. A representative of the laboratory will sign for the evidence including their name, date and time the evidence was received.
2. The laboratory representative shall ensure all needed documentation is delivered with the evidence. This includes the lab request form, search authority paperwork, and police reports.
3. The evidence will be inventoried and documented on an incoming evidence form.
4. The evidence will be wiped down and cleaned (if appropriate and only if no latent fingerprinting is requested).
5. The evidence will be properly sealed if not delivered in that condition.
6. The evidence will be entered into the computer evidence system and labeled.
7. The evidence will be secured within the property/evidence room within the laboratory.
8. If this is a new case for the laboratory a case number will be created and the case jacket forwarded to the lab director for prioritization.
9. The exact date and time the evidence is received is critically important to document for chain of custody issues. Anyone involved in the chain of custody for evidence should be prepared to testify in a court of law about his or her participation in the case.

**201.4 EVIDENCE HANDLING WITHIN THE forensic lab**

Forensic examiners will often have the need to retrieve evidence from the property/evidence room as part of their investigation. Evidence should be in the lab for only the absolute time necessary to conduct the examination and then be returned to the property/evidence room. While not always practical, evidence should not be left in the lab overnight or during weekend hours.

201.4.1 PROPER SEAL

All evidence stored within the Property/Evidence room shall be under proper seal. The seal shall be done in such a way that any opening or tampering with would be immediately obvious. Proper seals include such things as heat sealing and evidence tape. All seals will be initialed and dated by the individual sealing the evidence.

201.4.2 OPENING SEALED EVIDENCE

Sealed evidence should only be opened during the examination of evidence or when additional information is needed about the evidence (serial numbers, etc.). When opening sealed evidence care should be taken to leave the original seal intact if possible by creating a new opening in the packaging. Once finished with the evidence it shall be sealed as soon as possible, creating a new seal, which will bear the initials and date of the person responsible.

201.4.3 LABELS

All pieces of digital evidence stored by the laboratory will be bar-coded and entered into the evidence software application. Barcode labels will be affixed to each piece of evidence or the evidence bag they are stored in which will have the case number and the individual item number on it.

A bright green “Do not handle without gloves” label will be affixed to any evidence that must be handled with gloves due to latent prints or other reasons. An orange “Biohazard” sticker will be affixed to any evidence, which has bodily fluids or other biohazard substances on it. A green “Ok for release” sticker will be affixed to evidence once the forensic examiner has completed an exam on the item and it is no longer needed. This notifies the property/evidence specialist that the evidence can be released back to an originating agency.

201.4.4 CHAIN OF CUSTODY

Anytime evidence is removed from the property/evidence room the chain of custody form for that case number shall be updated. Each case that has evidence associated with it will have a printed chain of custody form within the case jacket. The person removing the evidence will indicate the date/time of when the evidence was removed, why it was removed and the date/time of when it was returned to the property/evidence room.

**201.5 RELEASE OF DIGITAL EVIDENCE – LABORATORY**

Evidence that is seized by the laboratory in our own investigations shall be stored within our own secure property/evidence room.

* If evidence is seized by consent and the person who possesses control over the evidence revokes consent, immediate arrangements should be made to return the evidence. The owner must sign that they received the evidence.
* Evidence that is seized pursuant to a search warrant will be kept within the evidence room until released by the lab director. Prior to release the prosecutor responsible for the case will be consulted.
* Evidence that contains contraband such as child pornography will not be released at any time to anyone who is not a law enforcement agent. Exceptions will only be made pursuant to a court order and permission of the lab director.

**201.6 RELEASE OF DIGITAL EVIDENCE – OUTSIDE AGENCIES**

The laboratory does not store property/evidence on a long- term basis for any agency. Once the forensic examiner assigned to the case is confident the original evidence is no longer needed, the case agent should be contacted to retrieve the evidence.

At times agencies may request that we release property/evidence directly from our facility to a suspect or involved party. This should be avoided whenever possible, and will only be done with prior approval from the lab director. Release of evidence that contains inappropriate images or contraband will not be released to anyone other than the originating law enforcement agency.

When releasing evidence back to the originating agency, the following procedure shall be followed:

1. The representative from the originating agency will sign showing receipt of the evidence. This must document their name, the date, the time, and what evidence items they are collecting.
2. It is common for items of one case to be released at different times. It must be made clear on the evidence inventory form what items are release and when.
3. The bar code labels on the evidence must be scanned in and shown as released to agency in the computer evidence program.

**201.7 RELEASE OF EVIDENCE – CONTRABAND**

Any evidence that contains contraband will be properly labeled as such using the bright red stickers in the property/evidence room stating, “Do Not Release – Contains Contraband”. When evidence that contains contraband is released to an outside agency, they shall be notified verbally and must sign the contraband acknowledgement form. This form will be maintained with the case jacket.

**201.8 DESTRUCTION OF EVIDENCE**

The laboratory is occasionally requested to destroy evidence after a case is adjudicated. Generally this is in child pornography cases, however can be for other criminal cases where evidence of the criminal activity is still accessible by a computer user. The laboratory will forensically sterilize digital evidence as a service to law enforcement agencies. No evidence will be destroyed without first having a court order or a signed consent form from an owner and approval from the lab director.

In cases where the laboratory is requested to destroy digital evidence a case number shall be pulled and a brief report will be completed. A report from a validated software program indicating that all sectors on the device have been overwritten would also suffice.

**201.9 EVIDENCE AUDITS**

A property/evidence support specialist shall audit the property/evidence room at six-month intervals. The property/evidence specialist will complete a memorandum and forward it to the lab director at the completion of the audit indicating the results of the audit and if any discrepancies were found and what actions were taken to resolve discrepancies.

The lab director will also complete at least one random audit per year and accompany the property/evidence specialist during the audit.

|  |
| --- |
| Policy 202 – Evidence Retention and Destruction |

**202.1 PURPOSE AND SCOPE**

This policy defines how evidence will be retained within the forensics lab, the length of evidence retention, evidence destruction, and responsibilities.

**202.2 EVIDENCE RETENTION**

202.2.1 IN-HOUSE EVIDENCE

Original Evidence seized by the laboratory will be maintained pursuant to state statutes and held until the case is adjudicated and the appeal period has passed. Certain cases may need to be kept for longer periods of time depending on the type of crime. Forensic images and other digital files from original evidence will also be maintained for the same amount of time as the original evidence.

202.2.2 OUTSIDE AGENCY EVIDENCE

Original evidence delivered by outside agencies will only be maintained in the property/evidence room until it is no longer needed by the forensic examiner. At the time the forensic examiner is finished with the original evidence it shall be returned to that agency for storage.

Forensic image files and other digital files from the original evidence shall be maintained by the laboratory until the original agency indicates in writing that the evidence is no longer needed. The support specialist is responsible for tracking evidence stored by the laboratory as well as obtaining written permission from case agents when evidence may be destroyed.

**202.3. RETENTION SCHEDULE**

Original evidence seized by the laboratory and digital image files and other related evidence from outside agencies shall be retained pursuant to state statue.

**202.4 DOCUMENTATION**

The Support Specialist will occasionally inquire with outside agencies about the status of cases to determine if the laboratory can purge digital evidence. The Support Specialist will send case agents either electronically or via traditional mail a “Case Disposition Status Request” memorandum. All returned forms, regardless of the status indicated shall be scanned and placed within the digital case file for the respective case. The case disposition status request form must be signed by the case agent or someone of authority from the originating agency. If a case disposition status request form is returned indicating that evidence can be purged, it shall be forwarded to the lab director for review.

**202.5 EVIDENCE DESTRUCTION**

If the lab director reviews the case disposition status request form and everything appears to be in order, s/he may authorize the destruction of digital evidence. This may include the deletion of forensic image files, exported data, FTK case information and any other evidence taken from the originally submitted evidence.

If any evidence is destroyed, the following shall be documented on the corresponding incoming evidence form:

1. Person who destroyed evidence
2. Date/time evidence was destroyed
3. Method of destruction (deletion, physical, etc.)

**202.6 RETENTION OF CASE REPORTS**

All case reports and information contained within the “Master Case File” shall be retained forever. This information is also backed up to tape on a daily basis.

|  |
| --- |
| Policy 203 – Physical Access |

**203.1 PURPOSE AND SCOPE**

The laboratory provides digital evidence forensics and investigative services to several law enforcement agencies. Many of the investigations are extremely sensitive and evidence stored in the lab must be kept in strict confidence. This policy establishes the requirements of laboratory personnel to maintain physical security of the facility.

**203.2 PERSONNEL RESPONSIBILITIES**

It is the responsibility of every laboratory member to ensure the safety and security of the facility. Personnel must make every effort to maintain security and ensure no unauthorized people enter the facility.

**203.3 PHYSICAL ACCESS AND SECURITY**

Individuals assigned to the laboratory will be issued an electronic key fob and PIN to access the facility. Laboratory members must use both the fob and PIN for authentication and access.

1. Sharing of key fobs or PIN’s is strictly prohibited and may result in a loss of access, removal from the laboratory, or other disciplinary action from the respective agency.
2. The laboratory is equipped with a burglar alarm system. Laboratory members who need:
   1. 24/7 access to the facility will be provided a PIN for the alarm system. The alarm shall be activated anytime the facility is unoccupied regardless of the time of day.
3. All doors within the laboratory shall be closed when the area is unoccupied.
4. Access to the laboratory is limited to members of the laboratory only.
5. Law enforcement officers, parole/probation officers and district attorneys may be allowed access to the facility without permission of the lab director, however they must be escorted at all times by a laboratory member.
6. Anyone who enters the laboratory facility past the front lobby is required to sign in and be issued a visitor badge which must be prominently worn during their entire stay. If anyone enters the laboratory area they must sign an additional log.
7. Defense attorneys, defense experts, maintenance people and others who are not part of the general public and have a legitimate need to enter the facility may do so, however must always be escorted by a member of the laboratory.
8. At no time shall anyone other than laboratory members be allowed to have unescorted physical access to the property/evidence room or the forensics area.

**203.4 ACCESS TO FACILITY BY VISITORS**

1. Visitors to the laboratory will first be met in the laboratory lobby. Visitors must sign in and be issued a visitor badge. Visitors may always be denied entry by a laboratory member if sensitive material is being examined or investigated or if laboratory operations dictate the need to deny entry.
2. Due to the sensitive and often graphic content being examined in the facility, prior to allowing access to any non-laboratory member an announcement will be made to alert all personnel of the incoming visitor.
3. In the event a laboratory member is bringing a visitor in with them, they must use the door intercom and receive permission from members inside the lab prior to allowing the visitor to enter.
4. Any law enforcement personnel may visit the lab and have access to the lab without prior approval. At no time will anyone be allowed inside the lab without the presence of a laboratory member.
5. No recording devices shall be allowed past the lobby of the laboratory except for sworn law enforcement officers on official business. All cellular phones, digital cameras, and other recording devices must be left just inside the lobby door and secured by laboratory members prior to allowing access to any visitor beyond that point. Although law enforcement may take recording devices into the lab area, they are not to record anything inside the lab without the permission of the lab director.

|  |
| --- |
| Policy 204 – Fire and Evacuation Plan |

**204.1 PURPOSE AND SCOPE**

In the event of an emergency requiring an evacuation, all laboratory members shall safely evacuate the building while ensuring the integrity of the facility as much as possible.

**204.2 FIRE ALARM AND EVACUATION PLAN**

In the event of afire alarm activation for the building all laboratory members shall immediately place any evidence within the forensic lab into the secure property/evidence room and evacuate. All interior doors of the forensic lab should be closed and the burglar alarm activated prior to leaving if possible.

In the event of a fire within the laboratory facility, fire extinguishers are placed throughout the facility. Laboratory members may attempt to extinguish small fires themselves if they feel it is safe to do so. If the fire is too large or too dangerous the laboratory member should immediately dial 9-1-1 and try to close as many interior doors as possible and immediately evacuate.

For other emergencies such as an earthquake or building collapse laboratory members must make a determination if evacuation or shelter in place will be the safest for them.

Evacuation plans are posted by the exits of the forensic lab and training room.

**204.3 NOTIFICATION OF SUPERVISOR**

At any time if the facility must be evacuated for any reason the lab director shall be notified as soon as practical.

|  |
| --- |
| Policy 205 – Facility Safety and Maintenance |

**205.1 PURPOSE AND SCOPE**

The laboratory strives to create a safe, professional, and functional facility for all laboratory members. It is extremely important to ensure the facility is always maintained in a safe manner and any safety issues be reported immediately.

**205.2 REGULATIONS AND INSPECTIONS**

The forensic lab may be inspected at least quarterly by the safety committee members. This inspection will be done to check for obvious safety hazards such as accumulation of combustible materials, improper storage of materials, falling/tripping hazards, electrical issues, lack of emergency lights or signage, lack of fire extinguishers and more. Any safety issue noted will be referred to the lab director for repair.

The laboratory will also comply with pertinent federal, state, and local health and safety regulations such as OSHA.

205.2.1 MATERIAL SAFETY DATA SHEETS (MSDS)

MSDS sheets are available within the reference book section of the forensic lab for all employees to review. An MSDS sheet will be kept for all chemicals within the facility.

205.2.2 FIRE EXTINGUISHERS

Fire extinguishers located within the laboratory facility will be inspected on a regular basis by facility maintenance personnel to ensure they have been serviced and ready for use at all times.

205.2.3 FIRST AID KITS

Located within the laboratory facility will be at least one plainly marked first aid kit and blood borne pathogens spill kit available to all members.

205.2.4 MANUAL

Laboratory members are expected to follow the health and safety rules and regulations of their individual agencies.

**205.3 REPORTING UNSAFE CONDITIONS**

It is the responsibility of each laboratory member to immediately report any unsafe condition they find to the lab director. If necessary the safety issue should be corrected by the laboratory member if possible. If the lab director is unavailable and the matter is urgent, the facilities maintenance manager should be notified.

|  |
| --- |
| Policy 206 – Health and Safety Program |

**206.1 PURPOSE AND SCOPE**

It is important that personnel can work in an area that is free from hazards or safety issues. Safety is the top priority of the laboratory and all personnel are considered safety officers with the duty to report safety issues and take action if unsafe conditions are found. This policy describes the health and safety program for the laboratory.

**206.2 HEALTH AND SAFETY MANAGER**

The Support Specialist shall assume the responsibility of the Health and Safety Manager.

**206.3 SAFETY INSPECTIONS**

The safety committee will conduct routine inspections of the facility to ensure compliance with all required statutes, ordinances, and regulations. A copy of the findings will be provided and maintained by the lab director.

**206.4 SAFETY COMMITTEE**

The parent organization of the laboratory has assigned one member of management to the safety committee and is the liaison between the laboratory and the safety committee.

**206.5 SAFETY EQUIPMENT**

The facility is equipped with two fire extinguishers in the forensics lab, one in the training/computer lab and two in the hallway outside of the lab. Laboratory members should be familiar with their operation.

The lab also is equipped with a first aid kit, blood borne pathogens kit and MSDS sheets. All employees shall know where these are at and should be able to access them at any time.

The lab provides latex gloves to all employees for use with evidence that may be dirty, contaminated with bodily fluids, or preserved for latent prints. Personnel should use latex gloves anytime they feel it is necessary. In addition, a hand sanitizing station is provided in the training room as is a sink with soap and water.

There is an AED (Automatic External Defibrillator) located adjacent to the forensics lab. All phones also have the ability to dial 9-1-1 in the event of an emergency.

**206.6 FIRST AID CERTIFICATIONS**

The lab director and at least one other member of the laboratory shall maintain a current First Aid/CPR card. Documentation of the card will be maintained within the employee training file.

# Chapter 3 – General Operations

|  |
| --- |
| Policy 301 – News Media Relations |

**301.1 PURPOSE AND SCOPE**

This policy provides guidelines for media releases and media access to the facility, criminal investigations, emergencies and other laboratory operations.

**301.2 RESPONSIBILITIES**

The ultimate authority and responsibility for the release of information to the media shall remain with the lab director. The lab director can designate another member of the laboratory with the responsibility of providing information to the media for certain events or investigations.

**301.2.1 MEDIA REQUEST**

Any media request for information or access to the laboratory facilities or regarding a laboratory investigation or operation shall be referred to the lab director, unless prior authorization has been given to another laboratory member. Prior to releasing any information to the media, laboratory members shall consider the following:

1. At no time shall any laboratory member make any comment or release any official information to the media without prior approval from the lab director.
2. In situations involving multiple law enforcement agencies, every reasonable effort should be made to coordinate media releases with the authorized representative of each involved agency prior to the release of any information by this laboratory.
3. Under no circumstance should any laboratory member make any comment(s) to the media regarding any law enforcement incident not involving this laboratory without prior approval of the lab director.

**301.3 SCOPE OF INFORMATION SUBJECT TO RELEASE**

The record of an arrest or the report of a crime shall be disclosed unless there is a clear need to delay disclosure in the course of a specific investigation, including the need to protect the complaining party or victim. Once the clear need to delay release is no longer present, the following information must be released:

1. The arrested person’s name, age, residence, employment, marital status and similar biographical information
2. The offense with which the arrested person is charged
3. The conditions of release
4. The identity and biological information concerning both the complaining party and the victim
5. The identity of the investigating and arresting agency and the length of the investigation
6. The circumstances of the arrest including time, place, resistance, pursuit, and weapons used
7. Such information as may be necessary to enlist public assistance in apprehending fugitives from justice
8. Information regarding the referral of juvenile offenders, or the victims of sexual abuse will be limited and only released by the lab director.

|  |
| --- |
| Policy 302 – Report Writing |

**302.1 PURPOSE AND SCOPE**

Report writing is a major part of all laboratory members’ job. The creation of a well written, organized, and detailed report is critical to the successful case resolution as well as maintaining an excellent reputation for both the laboratory member and the laboratory itself.

**302.2 REPORT PREPARATION**

Laboratory members are required to create a report for each case number that is created. All reports shall contain, at a minimum, information about the individuals involved in the investigation, all pertinent information seen, heard, or assimilated by any other sense, and all actions taken. Forensic reports must also include conclusions or opinions of the examiner about the evidence examined. Laboratory members shall not repress, conceal or distort the facts of any reported incident, nor shall any member make a false report orally or in writing.

**302.3 REPORT DOCUMENTS**

All case numbers generated shall have, at a minimum, a face sheet generated by the forensic examiner. If the details of the investigation can be completely contained within the summary space provided on the face sheet, then it will generally suffice as the entire report. Most often a forensic analysis report will accompany the face sheet.

In the event that a case is adjudicated prior to the forensic examination being completed on evidence, or the submitting agency cancels the request a full forensic examination report is not required. A face sheet is still required and the examiner must document the circumstances of why a full examination was not completed and submit the face sheet to the lab director for review and approval.

Laboratory members shall always use the appropriate laboratory documents and forms when completing paperwork.

The final analysis report shall be completed on the laboratory report form and will include the following information at a minimum:

1. Laboratory Case Number
2. Originating Agency Case Number
3. Name of Case Agent
4. Suspect Name (if known)
5. Evidence Submitted
6. Date and Time Report Created
7. Examination Conducted
8. Summary of Analytical Results
9. Disposition of Evidence
10. Handwritten or Digital Signature of Examiner

302.3.1 AUTHOR’S SIGNATURE

All reports created within the laboratory must bear the signature (either electronically or by hand) of the originating author of the report.

**302.4 SUPERVISOR APPROVAL**

Any report written by a laboratory member shall be forwarded to the lab director for review and approval. At no time shall any report be release outside of the laboratory prior to it being approved by the lab director.

If corrections are necessary to the report, the lab director will indicate what corrections need to be made and return the report to the author. Once approved, the lab director shall also sign the report (digitally or by hand) that the report has been approved and can be disseminated as needed.

All reports created within the laboratory by forensic examiners shall undergo a technical and administrative review by the lab director.

302.4.1 TECHNICAL REVIEW

100% of reports submitted by a forensic examiner will undergo a technical review by the laboratory director. The review will include the final report and any other supporting documents the examiner used to base their opinions on. The technical review will look for the following items:

1. All documentation is properly labeled.
2. Appropriate protocols were used.
3. The basis for the opinion is supported by the evidence found
4. The lab director agrees with the opinion of the examiner
5. All necessary examinations were conducted

20% of reports authored by the lab director will be technically reviewed by a forensic examiner within the lab.

302.4.2 ADMINISTRATIVE REVIEW

100% of reports will also be administratively reviewed by the lab director. An administrative review will consist of the following items:

1. All documentation is present and completed correctly
2. The report is free of grammatical errors
3. All reports and documents are sufficiently labeled

304.4.2 DOCUMENTATION OF REVIEWS

Reviews shall be documented within the disposition information section of the lab’s records management system.

**302.5 REPORTS CONTAINING CONTRABAND**

If a laboratory member is creating a report that contains images of child pornography or other contraband, that member shall also create an exact duplicate of the report except for the actual contraband images. This redacted copy of the report shall be provided to the investigator submitting the evidence or the attorney’s office.

**302.6 STORAGE OF REPORTS**

All computer generated reports within the laboratory shall be saved within the respective Master Case File on the server within the Master Case File. Handwritten reports, or other documents not generated by the laboratory shall be scanned in as an electronic document and stored electronically in the Master Case File.

**302.7 REPORT SECURITY**

Reports generated by the laboratory are stored on the secure server and cannot be accessed by anyone other than laboratory personnel who are authorized by the lab director. Reports shall not be shown or disseminated to anyone outside of the laboratory without the approval of the lab director.

**302.8 REPORT AMENDMENTS**

If a discrepancy is discovered in a report that has been issued, the report must be corrected and an amended copy provided to the case agent and customer. Amended reports are reviewed by the lab director prior to being disseminated. The following protocol shall be followed when amending a report:

1. When a discrepancy is found the lab director shall be immediately notified.
2. The section(s) that need amending shall be stricken with a single strikeout line through the affected areas.
3. After the stricken area the correct information shall be placed in the report.
4. The heading of the report shall be changed to “Amended Report” and the date of the amendment shall be included.
5. The amended report will be forwarded to the lab director for another technical and administrative review.
6. Once approved the amended report will be converted to a PDF document and bear the digital signature of the author, lab director and the approval stamp.
7. A new report shall be printed or burned to optical media.
8. A letter of explanation shall be written by the examiner on laboratory letterhead explaining the amendment.
9. The amended report shall be saved as: “AMENDED REPORT – (date of amendment)” within the Master Case File for the appropriate case and within the FINAL REPORTS folder.

**302.9 FINAL REPORTS**

Forensic examiners shall create their reports in Microsoft Word using the standardized template created for the laboratory. Once the report is completed, the case jacket shall be placed in the lab director’s box pending a technical and administrative review.

The lab director will conduct a technical and administrative review of the electronic copy of the Microsoft Word report and place any comments directly on the report using Microsoft’s commenting features. The examiner will then have an opportunity to correct any issues and will notify the lab director when the report has been corrected.

The lab director will review the report to ensure all issues were corrected and then notify the examiner to create the Adobe Acrobat version of the report and digitally sign the document. Once this is done the lab director will conduct an additional administrative review of the report and ensure the report is grammatically correct, formatted correctly and that no changes have occurred since the original technical review.

If the lab director approves the report, an “Approved” stamp will be placed on the last copy of the report along with the lab director’s digital signature. The report will then be locked by the lab director preventing any further changes and placed in the FINAL REPORT folder within the Master Case File folder on the server for that particular case. The report can be printed as a PDF document for distribution purposes.

Any report not containing the approved stamp and the digital signature of both the author and the lab director shall not be distributed outside the laboratory.

Final approved reports will be considered “completed reports” and cannot be modified once placed in the FINAL REPORT folder. In the event a report must be amended, or a supplemental report created for the same Master Case File, all versions must be appropriate named and stored. For example, for case #15-1234 has a final report, amended final report and a supplemental report. The file path would be as follows:

MASTER CASE FILES\HTCTF CR#15-1234, TYPE OF CASE – SUBMITTING AGENCY\FINAL REPORT\ Final Report.PDF

MASTER CASE FILES\HTCTF CR#15-1234, TYPE OF CASE – SUBMITTING AGENCY AMENDED REPORT - 03-01-15-Supplemental report.pdf

Any report ever placed within the FINAL REPORT folder must be maintained for version history. No file within the FINAL REPORT folder shall be overwritten with new data. A nightly backup of this directory also ensures version tracking and maintenance.

|  |
| --- |
| Policy 303 – Equipment Testing and Verification |

**303.1 PURPOSE AND SCOPE**

All equipment used by laboratory members in the forensic examination of digital evidence must be first validated to ensure it functions in a manner consistent with product specifications.

**303.2 REQUIRED VERIFICATIONS**

The following items must be verified prior to being used in a forensic examination:

1. Hardware write blocking devices.
2. Forensic imaging software.
3. Forensic examination software.
4. Forensic hardware devices.

303.2.1 PERSONNEL CONDUCTING VERIFICATIONS

All forensic verifications must be conducted by personnel assigned to the laboratory who conduct forensic examinations of digital evidence, or done under their immediate supervision.

303.2.2 VERIFICATION REPORTS AND APPROVAL

All verifications will be maintained in digital format on the laboratory server as well as printed out in the forensic verification book within the forensics lab. All verifications shall be reviewed by the lab director 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 director.

303.2.3 VERIFICATION PROCEDURES

Personnel conducting verifications will use the standardized report format created by the laboratory. 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.

303.2.4 MAINTENANCE VERIFICATIONS

Generally, hardware verifications need to be done only once to ensure they function correctly after they have been placed in service. If any piece of hardware has become damage, shows obvious wear, or any person in the laboratory has questions about its reliability another verification shall be done and documented on the device.

Software verifications must be redone anytime a major upgrade takes place for the software (such as FTK 4.2 to FTK 5.0 would require a new verification, however FTK 5.1 to 5.5 would not). If any person believes the software is not functioning properly or questions the results received a new verification shall be conducted.

Hardware write blockers shall be verified at least once annually to ensure their continued functionality.

|  |
| --- |
| Policy 304 – Master Case File Documentation |

**304.1 PURPOSE AND SCOPE**

All records pertaining to a case are to be maintained in the electronic Master Case File. The Master Case File resides on the lab’s server and is backed up to tape on a nightly basis. This policy describes the content and use of the Master Case File.

**304.2 CONTENTS OF MASTER CASE FILE**

Each case worked by the laboratory will have a Master Case File created. It is the responsibility of the Support Specialist to create the Master Case File folder on the lab’s server.

Master Case Files will first be organized by year, then by individual and unique case number. For example the file path for a Maser Case File may look like this:

“Master Case Files\2015\CR#15-0001 – TYPE OF CASE – SUBMITTING AGENCY”

Master Case Files will generally contain the following information:

* Lab request forms
* Incoming evidence forms
* Internal chain of custody forms
* Subpoenas
* Search warrants
* Examiner notes
* Correspondence related to the case
* Final reports

\* Note – the Master Case File only contains work product and analysis reports, but does not contain forensic images. Those are stored on a separate location.

**304.3 PAPER CASE JACKETS**

While the case is under investigation and lab work is pending a paper case jacket will be created by the Support Specialist. This folder will be labeled with the internal, sequential, and unique laboratory case number. While paper documents are being used such as the internal chain of custody form and examiner notes they are to remain in the paper case jacket. Once the case has been finished the entire case jacket will be submitted to the lab director for approval and the administrative/technical review. The lab director will review the paperwork in the case jacket and any electronic documents created in the Master Case File folder. Once the case is approved the lab director will initial and date the case jacket and submit it to the Support Specialist who will distribute the reports as needed and scan in all paper documents.

Once the case is closed the Support Specialist will scan any paper documents into the Maser Case File as PDF documents. All documents remaining in the paper case jacket will be destroyed by shredding.

**304.4 NAMING CONVENTION**

For each case generated within the laboratory a Maser Case File will be created. The folder will be stored on the SAN (Storage Area Network) in the following file path:

Master Case Files\Year of Case

All Master Case File’s shall be named in the same manner. The naming convention shall be as follows:

CR#xx-xxxx, TYPE OF CASE – SUBMITTING AGENCY

For example, a case may look like this:

CR#15-0001, NARCOTICS – FBI

**304.5 SECURITY AND ACCESS**

The Master Case Files may only be accessed by members of the laboratory. The server which they are stored on is configured to only allow access to those people deemed necessary by the lab director. This includes the lab director, Support Specialist, forensic examiners, and criminal investigators.

|  |
| --- |
| Policy 305 – Storage of Digital Evidence and Forensic Images |

**305.1 PURPOSE AND SCOPE**

This policy discusses how digital and electronic evidence is to be stored and retained by the laboratory.

**305.2 DIGITAL FILE CREATION**

Once a forensic examiner receives a case that requires them to forensically image digital evidence, a digital folder shall be created in the secure area of the laboratory Storage Area Network (SAN). Only forensic examiners and the lab director have access to this section of the SAN.

Forensic images and FTK processing files are stored within the folder titled, “FORENSIC FILES” on the SAN. Within the FORENSIC FILES folder are subfolders for each year.

When creating a new folder the examiner shall navigate to FORENSIC FILES\YEAR\ and then create their new folder. The name of the new folder shall consist only of the laboratory case number. Within this folder shall be a folder for each evidence item number associated with the case. The examiner shall make at least two additional folders within the evidence item folder, one containing the forensic image and the other containing the FTK processing files. If additional forensic software is used, additional folders shall be made (such as NetAnalysis, Encase, etc.) The folders are to be named IMAGE and FTK EXAM respectively.

For example, the file path may look like this:

FORENSIC FILES\2015\15-0001\15-0001 ITEM 1\15-0001 ITEM 1 IMAGE\

and

FORENSIC FILES\2015\15-0001\15-0001 ITEM 1\15-0001 ITEM 1 FTK EXAM\

Having each case in its own folder structure and strict adherence to this policy will eliminate the potential for cross-contamination.

While all forensic examiners can access the FORENSIC FILES portion of the SAN, only the lab director has the ability to delete anything within those folders.

**305.3 DIGITAL FILES AS EVIDENCE**

For the purposes of retention and documentation, a forensic image of a computer shall be considered as evidence and treated as such within the laboratory. Any other data, such as FTK processing files or exported files from the forensic image is not considered evidence, but work product and does not require the same level of evidence retention that forensic images do.

Forensic images of digital media will be maintained by the laboratory until we have been notified by the case agent that it is no longer necessary to store this. Written notification will be provided to the lab director indicating that the forensic images are no longer needed and all timelines have been exhausted pursuant to statutes. These written documents shall be signed by the case agent, scanned into PDF forms, and placed within the Master Case File for that particular case. Once permission has been received to remove the forensic images, the lab director shall be responsible for destroying the digital forensic images. Master Case Files and finished reports will be preserved forever.

For cases that must be retained, once the forensic examiner has completed the examination and it appears the forensic image may not be needed in the near future it may be backed up to tape and maintained within the lab. Tape backup is the long term storage solution for the laboratory.

|  |
| --- |
| Policy 306 – Release of Information |

**306.1 PURPOSE AND SCOPE**

Information may be requested from the laboratory by a variety of sources. This policy describes how different legal requests shall be handled.

**306.2 REQUESTS**

306.2.1 DISCOVERY

A request for discovery made directly to the laboratory will require the consultation of the opposing counsel. Only copies of documents will be provided upon a request for discovery and only after the approval of the laboratory attorney or opposing counsel.

306.2.2 SUBPOENAS

Forensic examiners must respond to subpoenas. If there is a scheduling conflict it is the responsibility of the forensic examiner to notify the client or subpoenaing party.

**306.3 PUBLIC INFORMATION REQUESTS**

Requests made under the public records laws will be forwarded to the lab director for review.

|  |
| --- |
| Policy 307 – Deviation from Policies and Procedures |

**307.1 PURPOSE AND SCOPE**

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.

**307.2 ACCEPTABLE DEVIATION OF POLICY/PROCEDURE**

In rare circumstances it may be necessary for a member of the laboratory 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 member to complete a thorough investigation.

**307.3 DOCUMENTATION REQUIRED**

In the event that written policies or procedures are deviated from by a laboratory member the justification for deviation and the circumstances surrounding the incident shall be documented within the case report. The lab director shall also be notified.

**307.3.1 REVIEW OF DEVIATIONS**

The lab director shall perform administration and technical reviews on any case where a deviation of policy or procedure took place. The lab director will also examine the policy and procedure that was deviated from and determine if updates or changes are warranted for that policy or procedure.

# Chapter 4 – Personnel

|  |
| --- |
| Policy 401 – Proficiency Testing |

**401.1 PURPOSE AND SCOPE**

All members of the laboratory who participate in the forensic examination of digital evidence must be proficiency tested at least once annually in all disciplines and at least every five years in all sub-disciplines they practice in to ensure they are properly performing their duties and maintaining knowledge of forensic procedures.

**401.2 TESTING METHODS**

401.2.1 LAB DIRECTOR

The lab director shall be annually tested by an outside independent agency to ensure he/she is maintaining and adequate level of knowledge and properly conducting the forensic examination of digital evidence. The lab director shall maintain the results of the proficiency test and a copy of the results will be provided to his/her immediate supervisor to ensure full disclosure of testing results.

401.2.2 FORENSIC EXAMINERS

The lab director shall administer annual proficiency tests to each forensic examiner within the laboratory. The lab director may create the test or purchase a test already created for such a purpose. Forensic examiners are not required to be tested by an outside agency and the lab director will grade the tests. The lab director may also choose to require forensic examiners to be tested by an outside agency and will review the findings of that agency. The test may include written or practical evaluations and the lab director will maintain the results.

**401.3 MAINTENANCE OF RECORDS**

All proficiency tests and results will be maintained by the lab director within the member’s training file for a period of five years.

**401.4 REMEDIAL TRAINING**

401.4.1 LAB DIRECTOR

In the event the lab director does not pass an external proficiency test their immediately supervisor will be contacted and the appropriate remedial training and/or other action will be done.

401.4.2 FORENSIC EXAMINERS

If a forensic examiner does not successfully complete a proficiency test the lab director will meet with that individual and discuss the outcome of the proficiency test. The lab director may arrange immediate remedial training and may also suspend the examiner from further work in any discipline until the examiner is able to pass the proficiency test or is removed from the laboratory.

|  |
| --- |
| Policy 402 – Personnel Records |

**402.1 PURPOSE AND SCOPE**

The lab director shall maintain a personnel file for each person assigned to the laboratory. The file shall be subdivided into the following categories:

* Personnel history (assignments, promotions, etc.)
* Commendations
* Complaints and counseling
* Training
* Proficiency testing

|  |
| --- |
| Policy 403 – Clothing and Attire |

**403.1 PURPOSE AND SCOPE**

Personnel within the laboratory must present themselves in a way that is professional while also being practical for the assignment. This policy applies to all members assigned to the laboratory.

**403.2 RESPONSIBILITIES**

It is the responsibility of each member to maintain their clothing and personal appearance in a professional and clean manner. The lab director will ensure that all members meet this policy and may suggest clothing replacements or require members to change clothing in the event something is worn that is clearly inappropriate or unprofessional.

**403.3 DAILY OPERATIONS**

For day to day operations laboratory members shall wear business casual attire. This may include a slacks with a laboratory polo shirt, button up shirt with a collar, department issued uniform or anything else that is approved by the lab director or the parent organization.

**403.4 PROHIBITED ITEMS**

The following items shall not be worn while on duty:

1. Open toed sandals or thongs.
2. Swimsuit, tube tops, or halter-top’s.
3. Spandex type pants or see-through clothing.
4. Distasteful printed slogans, buttons or pins.

**403.5 COURTROOM TESTIMONY**

Attire for courtroom testimony shall be in compliance with policy #104.

**403.6 AFTER HOURS CALL-OUT**

It is understood that laboratory members are frequently called out after hours to assist with investigations involving technology. Whenever possible laboratory personnel should wear slacks and a laboratory polo shirt, however depending on the urgency of the request and the location of the laboratory member when they were called it may be necessary for them to immediately respond in the clothing they have on at the time of the request.

|  |
| --- |
| Policy 404 – Complaints Regarding the Quality System |

**404.1 PURPOSE AND SCOPE**

In the event a laboratory member has a complaint regarding the quality system within the Digital Evidence Forensics Laboratory it is their responsibility to contact the lab director and notify him/her of the issue.

**404.2 RESPONSIBILITIES**

404.2.1 STAFF

In the event that a staff member within the Digital Evidence Forensics Laboratory has a complaint regarding the quality system within the laboratory they are to notify the lab director immediately via a written memo or email message. The written notification must include who is lodging the complaint, the details of the complaint and suggestions for remedy.

If the complaint concerns the examination of digital evidence, or the staff member finds that equipment is not functioning correctly which is affecting the results of an examination they are required to immediately stop their exam and contact the lab director.

404.2.2 LAB DIRECTOR

Upon receipt of a complaint regarding the quality system the lab director shall begin an investigation into the complaint and notify the complainant that it has been received. The lab director may meet with the complainant to work on solving the issue. When a resolution is found the lab director will notify the complainant and may share the results with other staff members if appropriate.

If it is determined that evidence was affected by the complaint the lab director shall cause an investigation which shall attempt to identify any potential cases which were affected and re-examine that evidence. If necessary, the lab director will also notify the submitting agency and prosecutor’s office of such an event.

All complaints will be maintained by the lab director in an electronic file.

|  |
| --- |
| Policy 405 – Personnel Complaints |

**405.1 PURPOSE AND SCOPE**

Complaints lodged against any member of the laboratory or regarding the work product of the laboratory shall be handled according to this policy. All personnel assigned to the laboratory has a duty to receive a complaint from anyone wishing to lodge one and forward it to the appropriate supervisor.

**405.2 COMPLAINTS ABOUT LABORATORY PERSONNEL**

In the event a complaint is made about personnel assigned to the laboratory, the complaint shall be taken and forwarded to the lab director. The complaint shall be investigated by the lab director.

**405.3 COMPLAINTS ABOUT THE LAB DIRECTOR**

If a complaint is received by a member of the laboratory about the lab director it shall be documented and forwarded to the laboratory director’s immediate supervisor for investigation.

**405.4 COMPLAINT INVESTIGATIONS**

Complaints about the quality of work or discrepancies of forensic findings shall be investigated by the lab director.

Complaints involving a policy violation, inappropriate conduct, or things of that nature shall be investigated jointly by the lab director.

Any major complaints received in the laboratory that allege improper forensic methodology, unethical behavior, or other issues involving character, or integrity will be brought up to the laboratory parent organization as well.

|  |
| --- |
| Policy 406 – Corrective Action |

**410.1 PURPOSE AND SCOPE**

This policy outlines the corrective action procedures to be followed in the event that discrepancies are reported either through the proficiency testing process or in casework. The goal of the correction action plan is to review the discrepancy, determine the event(s) that led to the discrepancy, and implement appropriate corrective measures.

**410.2 CORRECTIVE ACTION PROCESS**

When a discrepancy changes the conclusion of a report or a proficiency test, the following corrective action will be taken and the results filed with the lab director.

* The lab director is notified of the discrepancy.
* All casework for the examiner will be halted.
* The analytical documentation is thoroughly reviewed to determine what caused the discrepancy.
* Implement a corrective measure.
* Confirm that a return to compliance has been achieved by analyzing reference samples where appropriate.
* Review, where necessary, all casework relevant to the discrepancy to determine if the discrepancy is an isolated incident.
* Notify any outside agencies who may have received a report or work product affected by the discrepancy.

**410.3 MASTER CASE FILE DOCUMENTATION**

An analytical discrepancy and the corrective action that returns a system to compliance must be documented. The following elements must be summarized in the Master Case File:

* Who discovered the discrepancy?
* Who was the analyst involved?
* When did the discrepancy occur.?
* What was the nature of the discrepancy?
* Why did the incident happen (scientific explanation if available)?
* What was the name of the test method?
* What was the nature of the corrective action?
* How was a return to compliance confirmed?

**410.4 INVOLVED EXAMINER**

When there has been a discrepancy found in an examiner’s work the lab director will meet with the examiner and discuss the situation. If needed the lab director may require the examiner to undergo additional competency testing, proficiency testing or attend remedial training.