**YOUR LOGO HERE**

**Digital Forensics and Incident Response**

**Administrative 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**

[1. Purpose](#purpose)5

[2. Scope](#Scope)5

[3. Roles and Responsibilities](#Roles_and_Responsibilities)5

[4. Requirements](#Requirements)5

[Evidence Handling Procedures](#evidence_handling)6

[Legal Proceedings and Testimony](#legal_proceedings)6

[Case Triage, Assignment, and Prioritization](#triage_assignment_prioritization)6

[Physical Access](#physical_access)6

[Classified Spillage Cleanup Procedures](#spillage_cleanup)9

[Case Documentation and Reports](#case_documentation_reports)26

[Fraud / Waste / Abuse Investigations](#fwa_investigations)31

[Equipment Testing and Verification](#testing_verification)31

[Storage of Digital Evidence and Forensic Images](#storage_digital_evidence_forensic_images)31

[Master Case File Documentation](#master_case_files)31

[Deviation from Policies and Procedures](#deviation_from_policies)31

[Corrective Action Plan](#corrective_action_plan)31

**This page intentionally left blank.**

**1. Purpose**

The purpose of the Cyber Incident Response Team (CIRT) Administrative Manual is to provide personnel administrative procedures when performing their duties.

**2. Scope**

This document is applicable to all Cyber Security personnel who have CIRT responsibilities including, but not limited to; collection and preservation of digital evidence, incident response, cyber investigations, fraud, waste, and abuse investigations, or the forensic analysis of digital evidence. The individuals most impacted by this technical manual are those assigned to the CIRT, although other Cyber Security personnel may find themselves assisting with digital investigations and should be familiar with the presence of this document.

**3. Roles and Responsibilities**

|  |  |
| --- | --- |
| Key Role / Position Title | Responsibility |
| Cyber Security Personnel assigned to CIRT | * Apply the instructions detailed in this manual in the course of performing their duties. * Provide input into making updates or changes to this manual as needed. |
| CIRT Team (CIRT) Supervisor | * Maintain document control, including revision tracking. * Ensure the document is reviewed at least annually to account for technological and/or administrative changes. * Incorporate changes requested by CIRT personnel. * Provide input as necessary to document. |
| Cyber Security Manager | * Ensure document meets all legal, technical, and administrative requirements. * Final approval of document. * Provide input as necessary to document. |

**4. Requirements**

CIRT personnel are responsible for knowing and following the information contained within this manual. As a condition of working in CIRT, all personnel are required to read and obtain necessary clarification of these policies and procedures. 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. All personnel are responsible for keeping informed about revisions to this manual. All revisions will be provided to personnel.

|  |
| --- |
| **Evidence Handling Procedures** |

**1. Purpose**

CIRT receives digital evidence from a variety of sources in the course of conducting incident response and digital forensic investigations. This policy details the proper handling and storage of property and evidence when in the custody of [agency name] staff.

**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 or controlled by [agency name].

**3. Receipt of Digital Evidence**

Upon taking possession of digital evidence, the Cyber Security staff member shall do the following:

1. Immediately note the date and time the evidence was received and whom delivered the evidence (e.g., a person’s name or UPS, FedEx, etc.).
2. Insure the needed paperwork has been filed or is accompanying the evidence. This would include, at a minimum, a forensic services request form under most circumstances.
3. A [Agency Name] Internal Evidence Form is to be completed.
4. A [Agency Name] Chain of Custody Form is to be created and attached to the sealed evidence.
5. The evidence will be placed under proper seal if not already delivered in that condition.
6. The evidence will be properly labeled with the unique case number and individual evidence item number.

**4. Evidence Handling Within [Agency Name]**

Forensic examiners and incident responders will often have the need to retrieve evidence as part of their investigation. Evidence should only be out of secure evidence storage for only the absolute time necessary to conduct the examination. While not always practical, evidence should not be left out overnight or during weekend hours.

4.1 Proper Seal

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

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 resealing the evidence.

4.3 Labels

All pieces of digital evidence stored by [Agency Name] will have an evidence label affixed to either the evidence itself or the evidence bag it is stored within. The labels shall have, at a minimum, the [Agency Name] CIRT case number and the unique evidence item for that particular piece of evidence.

4.4 Chain of Custody

Anytime evidence is removed from the secure evidence storage, the chain of custody form for that case number shall be updated. Each case that has physical evidence shall have a chain of custody form generated and stored with the evidence. 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 the evidence was returned to the secure evidence storage.

**5. Release of Evidence**

Long-term evidence storage may be necessary when an investigation involves fraud, waste, or abuse or the digital evidence may be used in a future legal proceeding. No evidence shall be released from [Agency Name] CIRT without the approval of the CIRT Supervisor, or in their absence the Cyber Security Manager.

When releasing evidence to another enclave or agency (such as law enforcement), the below actions will be taken:

1. The evidence will be removed from secure storage and the internal chain of custody form will be updated to reflect it was removed in order to provide the evidence to another party.
2. The incoming evidence form shall be updated to reflect the exact items of evidence that is going to be released to someone else.
3. If the person receiving the evidence is local, have them sign the incoming evidence form, acknowledging they are taking possession of the indicated evidence items (maintaining the chain of custody). If the person taking possession of the evidence requests a copy of the incoming evidence form, provide them a copy.
4. If the evidence has to be shipped to the requestor, securely package the evidence and send them a copy of the incoming evidence form to sign as well as the chain of custody letter. The requestor will sign the incoming evidence form and send it back to [Agency Name] for our records.

**6. Destruction of Evidence**

6.1 Destruction of Information when Determined to not Contain Evidence

At times the [Agency Name] CIRT may seize digital evidence and at the conclusion of an investigation realize that the digital evidence is no longer needed. In these cases, the storage device containing the digital evidence shall be wiped using approved tools and readied for re-use on a new case.

6.2 Destruction of Information Containing Evidence

In cases where digital evidence was used as evidence in a criminal or administrative investigation, the evidence shall be maintained as long as required by [Agency Name] policy, applicable state law, or federal law. Prior to destroying any data that is related to an investigation, approval shall be given by [Agency Name] legal, the CIRT Team Lead, and the Cyber Security Manager.

If evidence is no longer needed due to an investigation being adjudicated and all of the above approvals have been obtained, the evidence shall be destroyed by securely deleting it or physically destroying the storage device it is contained on.

**7. Evidence Audits**

The secure evidence storage shall be audited by the CIRT Team Lead at least every six months. The results of the audit shall be documented in a memorandum and saved as evidence of the audit.

**8. Evidence Retention**

Evidence seized by Cyber Security will be maintained in accordance with federal laws, rules, regulations, policies, directives, and guidance from a variety of sources. The CIRT Supervisor is responsible for maintaining evidence properly and for coordinating the release, purging, and destruction of evidence. At no time shall evidence be released, destroyed, or removed from evidence control without the approval of the CIRT Supervisor. For the purposes of this policy, evidence is referring to both the original evidence as well as any forensic images or other data derived from original evidence.

8.1 Fraud/Waste/Abuse Investigations

In cases of fraud/waste/abuse that are non-criminal, but result in the discipline or termination of an employee, the evidence shall be maintained until such a time that legal counsel advise the evidence can be destroyed.

8.2 Criminal Investigations

In cases involving criminal investigations, evidence shall be maintained until the case is adjudicated and all appeal time lines have been exhausted. Prior to destroying any evidence in a criminal matter, concurrence must be obtained from the prosecutor in the case.

8.3 Documentation

In order to ensure cases are purged and because there is a finite amount of physical and digital storage space for evidence, the CIRT Supervisor shall inquire with the appropriate individuals about case status and seek permission to purge evidence. A “Case Disposition Status Request” form shall be sent to the case agents, legal counsel, prosecutor, or whoever has the authority to approve the destruction of evidence. All returned forms, regardless of whether or not the destruction of evidence was approved, shall be scanned and maintained within the master case file for the respective case.

8.4 Evidence Destruction

If the CIRT Supervisor reviews the case disposition status request form and authorization is received to destroy evidence, they may authorize the destruction of the digital evidence and the release of physical evidence. This may include the deletion of forensic image files, exported data, forensic software case information (e.g. Encase Reports and FTK Case Files) and returned original evidence back to the submitting agency or division. 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.)

8.5 Retention of Case Reports

All case reports and information contained within the Master Case Files shall be retained forever.

|  |
| --- |
| **Legal Proceedings and Testimony** |

**1. Purpose**

Testifying in legal proceedings is one of the most important functions performed by CIRT members. Due to the sophistication and technological content of CIRT testimony, it is critical that members understand the importance placed upon their testimony and forensic findings. CIRT members shall always be truthful and exhibit professionalism while testifying in any legal matter.

**2. Personnel Responsibilities**

CIRT members are responsible for providing truthful, factual, and relevant testimony during legal proceedings.

**3. Preparation**

CIRT members may testify in a wide range of legal matters ranging from unemployment hearings to criminal trials. CIRT members should begin preparing for their testimony upon receiving notification of a pending hearing or trial. This preparation should include working closely with the [agency name] attorney or government prosecutor to determine what the issues are for the proceeding and what will be expected of the CIRT member.

The CIRT member should determine what the direct testimony questions might include and work with counsel to determine potential cross-examination questions and issues. Additional forensic analysis may need to be accomplished and demonstrative exhibits may also need to be created for the proceeding.

If the CIRT member may be submitted to the court as an expert witness, the CIRT member shall have a curriculum vitae (CV) available to provide to the court and opposing counsel.

**4. Working with Opposing Counsel**

If a CIRT member is contacted by the opposing counsel of a legal matter, that CIRT member shall immediately contact the CIRT Supervisor and the agency’s legal representation. The production of information or discovery shall be done in strict coordination and with the written permission of [agency name’s] legal counsel.

**5. Attire**

Each jurisdiction and type of legal proceeding is different and the CIRT member should consult with the CIRT Supervisor and the [agency name’s] attorney for guidance on proper attire. Business casual shall always be the minimum dress for any legal proceeding. If the CIRT member is to testify in a criminal hearing, grand jury, or trial the CIRT member shall wear a suit.

**6. Testimony Evaluation**

Courtroom testimony of CIRT members is evaluated by the CIRT Supervisor. The CIRT Supervisor may attend proceedings and watch the testimony of CIRT members and/or send a *Courtroom Testimony Evaluation Form* to officers of the court.

|  |
| --- |
| **Case Triage, Assignment, and Prioritization** |

**1. Purpose**

This policy defines how cases are triaged, assigned, and prioritized by [agency name]. This policy applies to all CIRT members.

**2. Personnel Responsibilities**

The CIRT Supervisor is responsible for the intake, triage, assignment, and prioritization of investigations based upon the facts known about each case. The CIRT Supervisor may change the assignment or prioritization of cases when new facts are discovered which necessitates a change. CIRT members are responsible for working their assigned cases and keeping the CIRT Supervisor updated with information about their cases.

**3. Case Prioritization**

Cases will be prioritized as set forth below for processing and examination:

1. Matters involving or affecting national security;
2. Imminent credible threats 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. Classified spillage cases or other leaks of classified information;
5. Imminent credible risk of loss of or destruction to data of significant value;
6. Immediate pending legal proceeding, or non-extendable, outcome-determinative legal deadline;
7. Confirmed compromise of host computer(s) within the enterprise;
8. Active exploitation attempts against [agency name] resources;
9. Investigations into the fraud/waste/abuse of government resources by employees, contractors, subcontractors, and other individuals.

**4. Exceptions and Modifications to Case Prioritization**

Under special circumstances and on a case-by-case basis, the CIRT Supervisor may authorize a case to be investigated outside of its normal prioritization classification. The reassignment will only be for the duration of the exigent circumstance.

**5. Assignment of Cases**

Generally, cases shall be assigned to CIRT members at the discretion of the CIRT Supervisor on a rotational basis. There may be times, however that cases are assigned to certain CIRT members based upon their unique level of experience, or in cases that require specific qualifications of the examiner (e.g., Secret or Top Secret clearance, Foreign Intelligence Surveillance Act (FISA) disclosures, etc.) which will be specifically assigned by the CIRT Supervisor.

|  |
| --- |
| **Physical Access** |

**1. Purpose**

The [agency name] CIRT performs digital forensic analysis and investigations that are sensitive in nature. Digital evidence, forensic equipment, and access to forensic reports and other artifacts must be controlled to maintain strict confidentiality and authenticity of information. This policy is specifically addressing access to unclassified protected areas. Any investigations or analysis conducted on classified systems within a classified space is already covered within [agency name] policies regarding access to classified areas.

**2. Personnel Responsibilities**

It is the responsibility of every CIRT 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.

**3. Physical Access and Security**

Employees of the [agency name] CIRT have undergone a federal background investigation and possess an active Top Secret clearance. Their HSPD-12 badges must be worn at all times. Physical security of the facility is provided by [name] subcontractor who provide armed guards at all gates. They can be contacted anytime there are suspicious circumstances.

Any government visitor with the appropriate badge and clearance may visit the CIRT facility with an escort from the team.

Non-government visitors or visitors without a HSPD-12 badge must go through the visitor process with [agency name] and arrive at the badging office. Once cleared to access the facility, the visitor must be accompanied by a Cyber Security staff member at all times while in the Cyber Security Office.

The prohibited articles policy is in effect at all times for the Cyber Security Office. Employees and visitors are not allowed to take any photographs without a photo permit, possess radio transmitting devices, weapons, and other items listed on the prohibited article policy.

**4. Evidence Storage**

The secure evidence storage of the Cyber Security Office is only to be accessed by [agency name] CIRT members and other individuals specifically authorized. An entry/exit log is maintained at the property/evidence control facility and all access must be documented.

|  |
| --- |
| **Classified Spillage Cleanup Procedures** |

**1. Purpose**

The purpose for this desktop instruction is to inform the reader of the proper methods to perform a classified spillage cleanup. Classified spillage occurs when information, which is classified, is processed or transmitted through an unclassified system. This information can be generated at other sites and sent to the [Agency Name], or can be something generated locally.

**2. Requirements to Begin an Investigation**

Prior to commencing any classified spill investigation, the CIRT Supervisor must be notified. Generally, the CIRT Supervisor will designate the lead Cyber Security Cyber Incident Response Team (CIRT) member who will remediate the spillage. The CIRT Supervisor is responsible for briefing the Cyber Security Manager and any other levels of management.

1. The investigator will have the clearance to work with the information level and category of the spill.
2. The investigator will have login accounts with access privileges sufficient to search for the spillage and to remove the spilled data. If another person will assist in the cleanup, that person will have the clearance to work with the information level and category of the spill.
3. The investigator will have an account on the [agency name] Secure Network (SN). Notes and case details will be stored here. The investigator will use this account to generate the After Action Report. The investigator will have the report reviewed by a Derivative Classifier will be used to determine if it is still classified or is OUO prior to dissemination of the report.
4. The investigator will have access to the media, whether it be desktop computers, network attached storage (shared drives), external drives, flash drives, email servers, IPN email gateway logs, server logs, and backup logs. Where the investigator does not have access, the investigator will open Remedy tickets to access IT support.
5. The tool and program arsenal include, but are not limited to: Encase Enterprise, FTK Imager, Microsoft SDelete, DBAN v1.6, Microsoft PS Tools, Dameware Mini Remote Control Console (DWMRCC), scripting tools, Tableau write blockers, and Tableau TD2 Forensics 1:2 Duplicator.

The approved methods to clear (overwrite) files are the Microsoft SDelete application. Files will

be overwritten using the three pass (-p 3) option. After all files have been cleared, the drive free

space will be overwritten with three passes using the zero (-z) option.

**3. Notification of an Incident**

3.1 Receiving the notification

Notification of an event can come from multiple sources. These sources can be, but are not limited to: Federal oversight - Cyber Security Office Manager (CSOM) or to the Designated Approving Authority (DAA), [Agency Name] Safeguards and Security group, [Agency Name] IT CIO, [Agency Name] Cyber Security Manager, direct-report from [Agency Name] internal groups or Inquiry Officers at other sites.

The desired method is by receiving the case via a Remedy ticket. The case shall be entered with the title “Information Cleanup” and have the date, time, and name of the person alerting Cyber of the problem. It will not contain any actual information concerning the incident. The CIRT Supervisor will be notified of the incident.

**4. Collaboration with Safeguards and Security**

Generally spillage reports originate within Safeguards and Security and are reported to Cyber Security. In some instances, however a spillage may be discovered by Cyber Security or reported directly to Cyber Security, especially when the spillage solely involves digital files being processed or stored on an inappropriately classified system.

4.1 Notification of Safeguards and Security

In the event that Cyber Security is notified of a spillage by anyone other than Safeguards and Security, the CIRT Supervisor or the Cyber Security Manager shall immediately notify the Safeguards and Security Manager.

4.2 Coordination of Response

The remediation of classified spills is to be a joint effort between Cyber Security and Safeguards and Security. The CIRT Supervisor and/or the Cyber Security Manager should be in frequent communication with the Safeguards and Security Manager. Safeguards and Security is responsible for determining the classification of files and Cyber Security is responsible for locating and removing files that have been deemed classified. If Cyber Security locates additional documents or needs further clarification on the classification of files, they are to seek guidance from Safeguards and Security.

**5. Investigation**

Details of a classified spillage are classified at the level and category of the information spilled. The investigator must take care with their notes of the case details and of their investigation not to commit a secondary spill. The case notes need to transferred to the secure network at the earliest opportunities to prevent additional spillages. The notes are to be keyed into a log or scanned into a file on the secure network and then shredded in an authorized classified shredder. Any electronic artifacts created during the investigation and cleanup must be transferred to the secure network by CDROM (preferred) or by DVDROM. Any unclassified system creating these artifacts will have to be cleared (securely deleted, if less than 0.01% of media capacity) of the artifacts. After reading the CDROM into the secure network, the CDROM will be destroyed in an [ageny name]-authorized device.

At earliest opportunity, get with the Inquiry Officer to get the details of the spill. As much detailed information as possible needs to be collected as soon as possible. The below questions should be asked/answered in preparation for spillage cleanup:

1. Did [Agency Name] generate the information?

If NO – The generating agency is responsible for reporting the incident to HQ and providing follow-up for the status of the cleanup. [Agency Name] will report their status to that group.

If YES – [Agency Name] will be the lead for the cleanup effort. The Inquiry Officer is a member of the Safeguards and Security group. [Agency Name] will submit an initial Incident Report after the initial discovery. A final report will be submitted after the case is complete.

1. Who was involved in the incident?
2. Are all the involved individuals known, or will there be an ongoing investigation to determine who has had access?
3. How old is the spill?
4. Has the date-range of the spill been identified, or is identifying the date-range part of the ongoing investigation scope?
5. Do we know document names?

If classified – The filename must be transferred to Cyber via the secure network. Also, if the file names are classified, the full name cannot be used to run searches for the files.

Are these all the documents, or is it a partial set? Was the data copied to other locations or files?

1. Did it arrive by email?

Was the contamination by incoming email? Did it go to more people than was reported? Use the IPN email logs to answer these questions.

1. Did it leave by email?

Did the contamination leave the [Agency Name] enclave? Did it leave the complex? Search the IPN email logs for evidence of the spillage leaving the site.

1. Which systems is it on, or do we not know the extent it has spread?
2. Collect the system names for the known locations. If the spillage was on systems or in applications where more than the originally reported individuals have access, determine the set of individuals which could have accessed the material and could have made copies.
3. Was it put on network drives, or other shared resources?

What shared resources did the users have access to? Which did they use on a regular basis? This category includes items like the S drive or a remote site. Some groups have shared drives established just for them. There are groups with their own SAN.

1. Did anyone put it on a flash drive or an external USB drive?

When talking to the users, inquire if they have copies on external media such as CDs, flash drives, or external hard drives.

1. Was it put on any servers?

Did the spillage get put on any application servers or the SharePoint servers?

1. Did the user have Blackberry devices and other mobile devices (iOS, etc.)?

Determine if the user had a mobile device, such as a Blackberry, an IPad, or IPhone, that the spillage could have been transferred to.

|  |
| --- |
| **Case Documentation and Reports** |

**1. Purpose**

Proper documentation of incident response activities is an essential part of CIRT responsibilities. The creation of a well written, organized, and detailed report is critical to the successful outcome of any investigation. This desktop instruction details the proper documentation of CIRT activities.

**2. Personnel Responsibilities**

Any Cyber Security staff member who performs incident response or investigative activity may be required to document their actions in a report. All members of the CIRT team have additional requirements to document incident response activities.

**3. Report Format**

[Agency Name] has developed standard report templates to be used for incident response investigations and digital forensic examinations. These report templates shall be used by Cyber Security personnel while writing reports.

**4. Report Guidelines**

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. [Agency Name] employees shall not repress, conceal, or distort the facts of any reported incident, nor shall any Cyber Security member make a false report orally or in writing.

**5. Report Documents**

Every investigation done by CIRT shall be logged in the [Agency Name] CIRT Case Database and an internal [Agency Name] CIRT case number will be assigned. Case numbers are assigned by the calendar year and then the numeric number of that case for the year (e.g., the 105th case in calendar year 2013 would have the [Agency Name] case number of 13-0105).

The majority of cases reviewed by CIRT will be sufficiently documented within the CIRT Case Database. CIRT members are required to complete the case details section and the resolution remarks with as much detail as possible.

There are instances when the CIRT Case Database will not provide adequate documentation and a full report will have to be completed. Mandatory activities which require a full report be generated include, but are not limited to:

1. The forensic examination of digital evidence.
2. A large-scale or APT response.
3. Any internal investigation that may result in discipline.
4. All fraud/waste/abuse cases generated by Legal, Internal Audit, Employee Relations, or Human Resources regardless of the findings during the investigation.
5. Any other time as required by the CIRT Team (CIRT) Lead or the Cyber Security Manager.

5.1 Author’s Signature

All reports created within [Agency Name] CIRT must bear the signature (either electronically or by hand) of the originating author of the report.

**6. Report Approval**

Any report written by [Agency Name] CIRT shall be forwarded to the CIRT Team Lead for review and approval. At no time shall any report be released outside of the Cyber Security Office prior to it being approved.

6.1 Peer Review

All incident response and digital forensic reports shall be peer reviewed by another CIRT member. The peer reviewer will review the report looking for the use of proper procedures and if generally accepted techniques were used during the investigation. The peer reviewer shall also ensure they agree with the conclusion(s) or opinion(s) offered by the original author of the report. A peer reviewer can request access to evidence in order to attempt to recreate certain events or do additional analysis. Peer reviewers should provide their feedback to the original author and can suggest additional investigative steps as necessary. The name of the peer reviewer shall be documented within the [Agency Name] Case Database. The peer review is designed to 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. All necessary examinations were conducted.

6.2 Administrative Review

Every report generated by [Agency Name] CIRT will also undergo an administrative review by the CIRT Supervisor. It is acceptable to have the CIRT Supervisor conduct both the peer review and the administrative review of a report. If the CIRT Supervisor is the original report author, they must have another CIRT member peer review their report, however the CIRT Supervisor can administratively review their own report. All administrative reviews shall also be listed in the [Agency Name] Cases Database.

The administrative review is designed to look for the following items:

1. All documentation is present and completed correctly.
2. The report is free from formatting and grammatical errors.
3. All reports and documents are sufficiently labeled.
4. The CIRT Cases Database has been properly completed.

6.3 Report Corrections

Reports will be submitted for peer review and administrative review in Microsoft Word format. Peer reviewers and the CIRT Supervisor will document any suggested changes on the report by either tracking changes or by using the reviewing features built in to Word. Once all corrections have been made, a final draft will be submitted to the CIRT Supervisor for another review. Once approved by the CIRT Supervisor, the report author will convert the report to PDF and digitally sign the report using Adobe Acrobat and their Entrust credentials.

The signed PDF version will be sent to the CIRT Supervisor for their approval signature. Once a report has the CIRT Supervisor approval signature, it can be distributed outside of Cyber Security as necessary.

**7. Storage of Reports**

All reports and related artifacts shall be stored within the Master Case Files for the unique case number related to the investigation. If artifacts are not in digital format, the CIRT member shall ensure the documents are scanned and placed into the appropriate case folder in the Master Case Files. Due to the nature of the investigations conducted by CIRT, reports shall have limited access and only be accessed on a need-to-know basis.

**8. Final Reports**

All final reports (reports in PDF that have the original author and approver digital signatures) shall be stored within a directory labeled “Final Report” inside the Master Case Files. This allows for immediate retrieval of reports in the event a report is needed in the future and since only approved reports are placed in this directory, it is known that the reports stored within the “Final Report” folder are appropriate for dissemination.

An example file path for a report would be:

S:\Cyber Security\Incident Response\MASTER CASE FILES\2012\12-0105\Final Report\12-0105 Report.PDF

All other supplemental documents and the original Word report should be in the root of the case directory within the Master Case Files.

**9. Flow Chart of Report Creation**

See a flowchart example on the following page:

CIRT investigator creates draft report in Word

CIRT investigator sends encrypted report for peer review

CIRT investigator incorporates peer review comments

CIRT investigator submits report to CIRT Supervisor for administrative review

CIRT Supervisor provides feedback to CIRT investigator. Author incorporates CIRT Supervisor comments

CIRT investigator resubmits final draft report to CIRT Supervisor for final review

Once approved, CIRT investigator creates final PDF of report, digitally signs it and sends to CIRT Supervisor

CIRT Supervisor digitally signs report. Report is sent back to author for distribution.

Final signed PDF report stored within “Final Report” folder in Master Case Files

|  |
| --- |
| **Fraud / Waste / Abuse Investigations** |

**1. Purpose**

The purpose of this document is to detail the actions Cyber Security personnel should take when investigating a fraud, waste, and abuse (FWA) case.

**2. Personnel Responsibilities**

This document applies to all personnel within the Cyber Security Office that may be involved in the investigation of fraud, waste, and abuse cases. In particular, members of the Cyber Incident Response Team (CIRT) will be most likely involved in these investigations.

**3. Investigations**

Investigations of FWA cases typically involve a suspicion that an employee is engaging in activities that are defrauding the government, wasting government resources, or abusing resources provided to them. Cyber Security is called upon to investigate individuals who may be abusing their access to technology items or defrauding the government via technology. Some examples of FWA cases that Cyber Security becomes involved in includes, but is not limited to:

1. Using government equipment for excessive personal use.
2. Using government equipment to defraud the government.
3. Using government equipment to spread rumors, gossip, or libelous statements.
4. Using government equipment to bully, harass, or intimidate others.
5. Using government equipment to access inappropriate material such as racist websites, hate websites, or adult material (e.g. pornography).

FWA investigations are extremely sensitive and must be treated with complete confidentiality. Unless an employee has a direct need to know about the status of an investigation, information should not be disclosed to them. This includes other members of the Cyber Security Office.

As with all forensic investigations conducted by the Cyber Security Office, the employee who is assigned to lead the investigation must be completely unbiased and report only factual information about what is revealed during the investigation. Any employee who is assigned a FWA investigation must notify their supervisor immediately if they have any personal relationship with the employee who is under investigation or if there are any circumstances which may imply a conflict of interest.

Due to the sensitivity of FWA investigations and the potential consequences to the accused employee as the result of the investigation, the Cyber Security Office must follow this document when involved in these investigations.

**4. Fraud/Waste/Abuse Investigative Steps**

All requests for FWA investigations must be routed through the CIRT Team (CIRT) Lead. If another Cyber Security Member receives a request for an investigation, they shall direct the inquiring person to the CIRT Supervisor.

No investigation is to begin prior to all of the necessary paperwork being completed and approval received to initiate an investigation.

The CIRT Supervisor or their designee will send a Forensic Services Request Form to the person making the request for investigation.

FWA investigations will not commence until approval is received from [Agency Name] management. This approval may come from internal audit, human resources, employee relations, legal, or enterprise resources. At least one of the aforementioned departments must approve an investigation before it begins. In addition it is mandatory that the CIRT Supervisor and Cyber Security Manager approve the investigation. The only exception is if the investigation involves the CIRT Supervisor and/or Cyber Security Manager. In that case, the Chief Information Officer (CIO) must approve.

It is the responsibility of the CIRT Supervisor or the Cyber Security Manager to make the necessary notifications and obtain approval to initiate an investigation. Due to the complexity and sensitivity of these investigations, additional people may be notified as dictated by the facts of the investigation. Under no circumstances will the Cyber Security Office initiate a FWA investigation just upon the request of a department supervisor or manager without first receiving approval from another department list above (e.g., legal, internal audit, etc.).

If the investigation is approved, the CIRT Supervisor or their designee will create an internal [Agency Name] CIRT case number and create a folder within the Master Case Files. This folder will contain the completed forensic services request form as well as all artifacts and reports of the investigation. The CIRT Supervisor will assign the case to the appropriate Cyber Security Office personnel, or may conduct the investigation themselves.

If the case is assigned to a Cyber Security staff member, that employee will keep the CIRT Supervisor advised of the progress of the investigation and any major developments. Any requests for information regarding the progress or status of the investigation should be directed to the CIRT Supervisor or Cyber Security Manager.

A thorough report will be completed for any FWA investigation, regardless of the outcome or findings. This report will be peer-reviewed and approved prior to being distributed to anyone outside of the cyber Security Office.

4.1 Law Enforcement Involvement

In the event that law enforcement becomes involved in an investigation, all communication between the law enforcement officials and the Cyber Security Office will be done through the CIRT Supervisor or the Cyber Security Manager.

If, during the course of an investigation, a member of the Cyber Security Office determines there is evidence of a crime on a device being forensically examined they are to immediately stop the investigation and notify the CIRT Supervisor or Cyber Security Manager.

**5. Priority of Investigations**

FWA investigations are generally high priority incidents and the cyber component may be just one part of a multi-faceted investigation. Whenever practical, FWA investigations shall be done as expeditiously as possible for the benefit of [Agency Name] and the accused employee.

|  |
| --- |
| **Equipment Testing and Verification** |

**1. Purpose**

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

**2. Personnel Responsibilities**

This document applies to all personnel within the Cyber Security Office that may be involved in the forensic analysis of digital evidence.

**3. Required Validations**

The following items shall be validated 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.

**4. Personnel Conducting Validations**

All forensic validations must be conduced by personnel assigned to the CIRT who conduct forensic examinations of digital evidence, or done under their immediate supervision.

**5. Verification Reports and Approval**

All validation reports will be included in the [agency name] validation manual. Prior to being finalized, each validation paper must be approved by the CIRT Supervisor. All prior copies of forensic validations shall also be maintained within the CIRT SharePoint site (e.g., previous validations completed on older software versions).

**6. Validation Procedures**

Personnel conducting validations will use the standardized report formatted for [agency name]. All relevant fields on the form shall be completed as well as the expected and actual results of each validation test.

**7. Maintenance Validations**

Generally, hardware validations need to be done only once to ensure they function correctly after they have been placed into service. If any piece of hardware becomes damaged, shows obvious wear, or any person in the CIRT has questions about its reliability, another validation shall be done and documented.

Software validations must be done anytime a major upgrade is performed. [Agency name], in accordance with the DAA has defined a major upgrade as anytime the software version number to the left of the decimal changes. For example, FTK version 3.12 to version 3.14 would not require a re-validation. FTK version 3.x to version 4.x would require a re-validation.

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

|  |
| --- |
| **Storage of Digital Evidence and Forensic Images** |

**1. Purpose**

This policy discusses how digital evidence is to be stored and retained by the [agency name] digital forensics lab.

**2. Personnel Responsibilities**

This document applies to all personnel within the Cyber Security Office that may be involved in the analysis of digital evidence.

**3. Digital File Creation**

Once a CIRT member receives a case that requires them to forensically image digital evidence, a digital folder shall be created with the examiner’s partition on the forensic Storage Area Network (SAN). Forensic images and processing files (e.g. FTK or Encase files) are stored within a directory 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 CIRT 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 files and the other containing the forensic processing files. If additional forensic software is used, additional folders shall be made (such as NetAnalysis, RegRipper, etc.). The folders are to be named with the case number, evidence item number, and then a description of its contents. For example:

FORENSIC FILES\2013\13-0701\13-0701 ITEM 1\13-0701 ITEM I IMAGE\13-0701 ITEM 1 IMAGE.dd

Or

FORENSIC FILES\2013\13-0701\13-0701 ITEM 2\13-0701 ITEM 2 FTK EXAM\

Each filename and folder should contain the case number and the unique evidence item number it pertains to. This is done in the event that a folder is accidentally moved or misplaced, the examiner can quickly determine just by each folder name, what case it belongs to and move it back into the correct directory structure.

**4. Digital Files as Evidence**

For the purposes of retention and documentation, a forensic image of a digital device shall be considered evidence and treated as such. 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.

Forensic images of digital evidence will be maintained by CIRT until notification has been received that they are no longer needed. This notification may be received by case agents, attorneys, or others involved in an investigation that can provide written verification that an investigation is complete. Once approval has been received to purge any forensic images and all other timelines have been exhausted (statutes of limitations, legal actions, etc.), the CIRT Supervisor shall be responsible for destroying copies of forensic images. Written documentation shall be placed in the master case file indicating that the forensic images were destroyed along with the written notification from the case agent providing the approval for doing so.

|  |
| --- |
| **Master Case File Documentation** |

**1. Purpose**

All records pertaining to a case are to be maintained in the electronic Master Case File in accordance with [agency name’s] document management system. The Master Case File resides on the forensic server and is backed up on a nightly basis. This policy describes the content and use of the Master Case Files.

**2. Personnel Responsibilities**

All personnel who have access to the Master Case Files are required to follow this policy.

**3. Contents of Master Case File**

Each case investigated by CIRT will have an entry into the CIRT database and be provided with an unique case number. This case number begins with the calendar year and then the sequential number representing that particular case (e.g., 13-0854 is the 854th case in the calendar year 2013). Some cases may completely be documented within the database (such as a IDS/IPS alert that is determined to be a false positive), where other investigations will produce evidence and exhibits. Any case that produces additional documentation must have a corresponding Master Case File created to hold all of the relevant exhibits.

Master Case Files are also organized by year, then by individual case number. For example, the file path for a Master Case File should look like this:

Master Case Files\2013\13-0854\firewall logs.xls

Master Case Files will generally contain the following information:

* Forensic service request forms
* Incoming evidence forms
* Chain of custody forms
* Legal documents
* Communication and correspondence about the investigation
* Examiner notes
* Exported logs and other evidence
* Final reports

**4. Security and Access**

The Master Case Files directory is stored within the Cyber Security directory of a SAN and access control is limited using NTFS file permissions and active directory. Only members of Cyber Security and further only members of the CIRT can access these folders.

|  |
| --- |
| **Deviation from Policies and Procedures** |

**1. Purpose**

Due to the very nature of investigations involving technology and the ever-changing software, hardware, and analysis equipment, there may be time 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.

**2. Personnel Responsibilities**

This policies applies to all [agency name] CIRT members that perform digital forensic investigations.

**3. Acceptable Deviation of Policy / Procedure**

In rare circumstances it may be necessary for a CIRT member to deviate from the policies or procedures in place. The deviation may be due to an exigent circumstance or incidents where due to an articulated fact the standard policy or procedure would not allow the member to complete a thorough investigation.

3.1 Documentation Required

In the event that written policies or procedures are deviated from by a CIRT member, the justification for the deviation and the circumstances surrounding the incident shall be documents within the case report. The CIRT Supervisor shall also be notified.

3.2 Review of Deviations

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

|  |
| --- |
| **Corrective Action Plan** |

**1. Purpose**

This policy outlines the corrective action procedures to be followed in the event that discrepancies are reported either through testing or in actual 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.

**2. Corrective Action Process**

When a discrepancy changes the conclusion of a report, the following corrective action will be taken and the results filed with the CIRT Supervisor.

* The CIRT Supervisor is notified of the discrepancy.
* All casework for the examiner is 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 agencies who may have received a report or work product affected by the discrepancy.

**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 plan.
* How was a return to compliance confirmed.

**4. Involved Examiner**

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