

**Washington State
Department of
Social and Health Services**

**Information Technology
Security Procedures Manual**

**Revision 14.1
2015**

This procedures manual is meant for the exclusive use of DSHS personnel and business partners. Parts of this manual may be exempt from disclosure under the Public Records Act in RCW 42.56.420. Do not provide or disclose copies of this manual to anyone outside DSHS without consulting with the DSHS Chief Information Officer.

Chapter 2: Personnel and Use of State Resources.....	4
P2.2.8.S3 TERMINATED EMPLOYEES—DISABLING ACCOUNTS.....	4
Chapter 3: Classifying and Protecting Data and IT Resources	6
P3.2.4.S3 DATA SHARING CONTRACTS—COMPROMISE OF DATA SECURITY....	6
Chapter 4: Access Security, Identification, & Authentication	7
P4.2.4.1.S7 SECURE STORAGE OF ADMINISTRATIVE PASSWORDS	7
P4.2.4.1.S13 UNSUCCESSFUL LOGIN ATTEMPTS.....	7
P4.2.4.2 CONSTRUCTING PASSWORDS-- ADDITIONAL SUGGESTIONS	8
Chapter 5: Network, Operating Systems, and Internet Security	9
P5.2.3 PATCH MANAGEMENT PROCESS	9
A. Applicability.....	9
B. Software Inventory; Vulnerability Identification	9
C. Timeframes by Severity Level	9
D. Assessment, Testing, Implementation, Notification, and Documentation	10
P5.2.9.G1 WARNING BANNER—SAMPLE	10
Chapter 6: System Design, Development, Maintenance, and Operations.....	11
P6.2.1 INPUT RELATED SECURITY REQUIREMENTS	11
Chapter 8: Encryption and Data Integrity	12
P8.2.1.S1 ENCRYPTION OF CONFIDENTIAL INFORMATION REQUIRING SPECIAL HANDLING	12
Chapter 10: Detecting, Reporting, and the Investigation of IT-Related Incidents	13
P10.2.2.S1 REPORTING SUSPECTED INCIDENTS.....	13
<i>Section P10.2.3.S2 was eliminated, and its contents moved to P5.2.9.G1 (Revision</i> <i>11).</i>	14
P10.2.3.S3 ACCESSING EMPLOYEES’ FILES.....	15
P10.2.4.S2 PROTECTING CONFIDENTIALITY DURING AN INVESTIGATION	15
P10.2.4.S3 THE TWO PERSON RULE.....	15
P10.2.4.S4 CHAIN OF CUSTODY	16
P10.2.4.S5 SUSPECTED CRIMINAL ACTIVITY	16
P10.2.4.S7 IT SUPPORT FOR INVESTIGATIONS	16
Chapter 11: Safeguarding Federal Information	20
P11.3.2.S8 DESTRUCTION OF DOCUMENTS CONTAINING IRS TAX INFORMATION.....	20
P11.4.1.S4 PROCESSING “HIT” INFORMATION BY QA FIELD OFFICE	Error!
Bookmark not defined.	
Documenting "Hit" Information by QA Staff in Field Offices	Error! Bookmark not defined.
Third Party Verification from Employers.....	Error! Bookmark not defined.
Third Party Verification from Financial Institutions ...	Error! Bookmark not defined.
Third Party Verification - CSO Use of the Documentation.....	Error! Bookmark not defined.
Returning “Hit” Information to Olympia for Destruction.....	Error! Bookmark not defined.

Chapter 2: Personnel and Use of State Resources

This chapter contains:

➤ P2.2.8.S3 TERMINATED EMPLOYEES—DISABLING ACCOUNTS

P2.2.8.S3 TERMINATED EMPLOYEES—DISABLING ACCOUNTS

Upon termination of an employee, the employee's Active Directory, RACF, VPN, and Secure E-mail accounts will be disabled as follows:

A. The employee's administration will do the following:

1. Supervisors and/or managers will promptly report terminations to IT or security staff who are responsible for disabling accounts, removing system or application privileges, and removing facilities access.
2. Responsible IT or security staff will disable the employee's accounts, in accordance with [DSHS IT Security Policy Manual standard 4.2.3.1.S4 General User ID Requirements](#); remove system or application privileges; and remove facilities access.

B. The Human Resources Division (HRD) will:

1. Create a weekly list, from the Human Resources Management System (HRMS), of terminated employees.
2. Send this list, each Friday, to (a) the Point of Contact for each administration, and (b) the Information System Services Division (ISSD).

C. The Administration will: within five days, disable accounts, remove privileges, and remove facilities access in any case where this has not already been done.

D. ISSD will: on the fifth day, disable any accounts that ISSD can administer, such as Active Directory or RACF accounts, which have not already been disabled, for any employee on the list.

Exceptions: where one of the exceptions described at [DSHS IT Security Policy Manual standard 4.2.3.1.S4.b General User ID Requirements](#) applies, **the employee's administration will** notify the Administration Point of Contact, and ISSD, in writing, of the reason for the exception, and neither the Administration, nor ISSD, will disable the accounts.

Chapter 3: Classifying and Protecting Data and IT Resources

This chapter contains:

➤ P3.2.4.S3 DATA SHARING CONTRACTS—COMPROMISE OF DATA SECURITY

P3.2.4.S3 DATA SHARING CONTRACTS—COMPROMISE OF DATA SECURITY

Upon notification of:

- A material breach or violation of the data security related provisions of a contract, or
- Any event that has resulted in a compromise or potential compromise of DSHS data e.g. loss or theft of a laptop computer, other computing device, or media;

the DSHS Contact or responsible manager must promptly report these events, within one business day of discovery, to the ISSD Help Desk, as described at [DSHS IT Security Procedures P10.2.2.S2 Reporting Suspected Incidents](#). The Help Desk will notify the DSHS Privacy Officer and the DSHS IT Security Administrator.

The DSHS Privacy Officer, IT Security Administrator, and other involved program staff will determine what further reporting or additional action is needed.

As appropriate, steps must be taken to address the violation, mitigate the loss, notify affected persons, and/or reduce the likelihood of future violations.

Chapter 4: Access Security, Identification, & Authentication

This chapter contains:

- P4.2.4.1.S7 SECURE STORAGE OF ADMINISTRATIVE PASSWORDS
- P4.2.4.1.S13 UNSUCCESSFUL LOGIN ATTEMPTS
- P4.2.4.2 CONSTRUCTING PASSWORDS-- ADDITIONAL SUGGESTIONS

P4.2.4.1.S7 SECURE STORAGE OF ADMINISTRATIVE PASSWORDS

Storage of administrative passwords is more critical than user passwords due to the level of access granted to administrators. While it is understood that there are some situations where administrative passwords may need to be stored outside of default, secure locations, (e.g. an administrator who has different passwords for various devices, and/or applications, where it isn't practical to remember all of the various hardened passwords) all steps must be taken to ensure password protection.

- A. Do not write down the passwords.
- B. Storage on a portable device, such as a USB thumb drive, must be encrypted, such that access to secured data (including access password) on the device is protected by a hardened access password, and the device must automatically lock access to secured data (so that there is no way to recover, requiring a re-format) after a certain number of invalid attempts is reached.
- C. A log must be kept of who has possession of the USB thumb drive.
- D. Alternate methods of authentication, other than passwords, are available. These include digital certificates, RSA tokens, and bio-metrics.

P4.2.4.1.S13 UNSUCCESSFUL LOGIN ATTEMPTS

After five attempts, the opportunity to enter the correct password should be:

- A. Suspended until reset by the Help Desk or system administrator;
- B. Temporarily disabled for no less than three minutes; or
- C. Disconnected if remote access is involved.

Section P4.2.4.1.S13-A was eliminated from this manual, and its contents moved to the DSHS IT Security Policy Manual, section 1.5 Effective Date, Note 1 (Revision 11).

P4.2.4.2 CONSTRUCTING PASSWORDS-- ADDITIONAL SUGGESTIONS

- A. Do not use cyclical passwords, i.e., changing only a letter or number or using the name of a month, each time a password change is required.
- B. Whenever possible, use passwords that are easy to remember. Examples include:
 - 1. A common word that has been modified with a special character, and/or a number, e.g. B@ndleader, or b@and1eader.
 - 2. An acronym you have made up e.g. MD\$1Cute could stand for "**My Dog Star(\$)** Is(1) **Cute**".
- C. In environments that require higher than ordinary assurance of password integrity, consider the following two alternatives:
 - 1. Make passwords fifteen characters long. Construct the first seven characters and the last eight characters as separate, difficult to guess passwords for reasons explained in the [DSHS IT Security References Manual, R4.2.2](#).
 - 2. Upgrade the Local Area Network to the Microsoft NTLM 2 authentication protocol, as described in Microsoft Knowledge Base article [Q239869 "How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT"](#).

You may also consider the Additional Suggestions from Microsoft at [DSHS IT Security References R4.2.4.2 Creating Strong Passwords](#).

Chapter 5: Network, Operating Systems, and Internet Security

This chapter contains:

➤ P5.2.3 PATCH MANAGEMENT PROCESS

P5.2.3 PATCH MANAGEMENT PROCESS

A. Applicability

This patch management process applies to:

- Software installed on all computing platforms (Microsoft, Novell, Solaris, etc.)
- All computers in service in DSHS or authorized to connect to DSHS networks, including:
 - Department owned laptops or other computing devices in the possession of DSHS users, whether or not connected to any network.
 - Computers owned and/or administered by employees or business partners (e.g. vendors, auditors, other state agencies) that are currently authorized to connect to a DSHS network.

This process does not apply to:

- Network devices such as routers and switches. These devices also require patching, and should be maintained accordingly, by the administration owning or supporting the particular device.
- Computers removed from service by a system administrator for repair or to be held in storage for future use. These computers must be patched **off-line** before being returned to service.

B. Software Inventory; Vulnerability Identification

Each DSHS administration will maintain an inventory of software deployed in the production environment and/or on networked computers, and will monitor publication of related vulnerabilities and patches.

C. Timeframes by Severity Level

The DSHS IT Security Unit will assign severity levels and mandatory timeframes to patches for Microsoft software using the following categories.

Level	Implementation
Critical	6 business days

Intermediate	20 business days
Informational	Optional

NOTE: Times are from point of notification

IT Security will also forward, to DSHS administration IT security administrators, patch information received from DIS/WACIRC about other software. Each DSHS administration will assign timeframes, not to exceed those set by DSHS IT Security, to all security patches applicable to software deployed.

NOTE: The criteria used as a guide by IT Security to assign severity levels is described at [DSHS IT Security References R5.2.3-A DSHS Patch Severity Levels](#).

D. Assessment, Testing, Implementation, Notification, and Documentation

Within the timeframes noted above, each administration must:

- Complete an assessment of the impact of each patch (i.e. do you need to apply this patch, to which machines, etc.).
- Complete testing on systems and applications maintained by the administration.
- Implement patches where appropriate, and take necessary steps to minimize the impact of the patch on applications supported by the administration.
- If unable to implement a patch within the required timeframe on more than 2% of servers or 2% of workstations, notify DSHS IT Security as soon as possible.
- Document the extent to which you succeeded in meeting the required timeframes, and, where applicable, the reasons timeframes were not met, and planned corrective action.

P5.2.9.G1 WARNING BANNER—SAMPLE

The following suggested language is based on a sample from the U.S. Department of Justice (per *Windows NT Security Step by Step*, step 3.2, The SANS Institute, 1999).

!!! WARNING!!! By accessing and using this system you are consenting to possible system monitoring for law enforcement and other purposes. Any unauthorized use of this computer system may subject you to criminal prosecution and penalties, or other disciplinary action.

Note: This section was moved here from P10.2.3.S2 (Revision 11).

Chapter 6: System Design, Development, Maintenance, and Operations

This chapter contains:

➤ P6.2.1 INTERNET BASED APPLICATIONS

P6.2.1 INPUT RELATED SECURITY REQUIREMENTS

The following applies to all applications

Reference: [DSHS IT Security Policy Manual, 6.2.1.S4.b and S11](#)

1. Employ input validation to prevent injection of malicious code.
 - a. Validate input to all input fields, including hidden fields.
 - b. Use code running on the server (as opposed to the client computer) to validate all user input. Code running on the client computer may also validate input data, but should not be relied on (because client code can be bypassed).
 - c. Use a validation process that identifies a set of safe characters or character combinations to accept, and rejects all other input.
 - d. Use stored procedures and/or parameterized queries to generate SQL query code.
2. Prevent buffer overflows by either of the following means:
 - a. Use managed code languages such as Visual Basic.NET, C#.NET, or Java that automatically provide bounds checking; or
 - b. For any use of non-managed code languages such as C or C++, or of untested DLLs or other components, ensure that bounds checking or data-size checking is done.
3. Encrypt cookies where appropriate, e.g. where they contain credentials.

Chapter 8: Encryption and Data Integrity

This chapter contains:

- P8.2.1.S1 ENCRYPTION OF CONFIDENTIAL INFORMATION REQUIRING SPECIAL HANDLING

P8.2.1.S1 ENCRYPTION OF CONFIDENTIAL INFORMATION REQUIRING SPECIAL HANDLING

Encrypt confidential information requiring special handling as required by applicable regulations.

State and federal regulations governing mental health services, alcohol and substance abuse services, protected health information, and Federal tax information have stringent safeguard requirements. Those regulations govern how encryption may be used to protect information.

An example is Internal Revenue Service (IRS) Publication 1075, which requires that tax information be encrypted when transmitted outside of the Local Area Network (LAN) on which the data resides.

Chapter 10: Detecting, Reporting, and the Investigation of IT-Related Incidents

This chapter contains:

- [P10.2.2.S1 REPORTING SUSPECTED INCIDENTS](#)
- [P10.2.3.S2 WARNING BANNER—SAMPLE](#)
- [P10.2.3.S3 ACCESSING EMPLOYEES’ FILES](#)
- [P10.2.4.S2 PROTECTING CONFIDENTIALITY DURING AN INVESTIGATION](#)
- [P10.2.4.S3 THE TWO PERSON RULE](#)
- [P10.2.4.S4 CHAIN OF CUSTODY](#)
- [P10.2.4.S5 SUSPECTED CRIMINAL ACTIVITY](#)
- [P10.2.4.S7 IT SUPPORT FOR INVESTIGATIONS](#)

P10.2.2.S1 REPORTING SUSPECTED INCIDENTS

NOTE: The following instructions generally address reporting at the agency level. Each administration should establish procedures for internal reporting.

EVENT	CONTACT or CONSULT
<p>Lost or stolen computers or computing devices and cell phones;</p> <p>Misplaced, lost, or stolen DSHS BlackBerry devices (report “immediately”, per DSHS IT Standards Manual, IT Standard: 8.4.1. BlackBerry Personal Digital Assistant Security Settings);</p> <p>Loss; theft; or unauthorized acquisition, access, use, or disclosure of data in any form (e.g. paper or electronic) that potentially includes confidential information;</p> <p>Theft of other IT equipment or IT resources;</p> <p>Significant breaches or attempted</p>	<p>In cases of theft, first contact the appropriate law enforcement agency to report the theft and request a copy of the police report for agency use.</p> <p>Contact the ISSD Service Desk at 1-888-329-4773, 360-902-7700, or e-mail ISSDservicedesk@dshs.wa.gov.</p> <p>Do this as soon as possible, but never later than one business day after discovery.</p> <p>The Service Desk will notify the DSHS IT Security Administrator.</p> <p>In addition, follow the reporting requirements described in Administrative Policy 9.01 Incident Reporting and any applicable policies or procedures of your administration.</p> <p>For Federal Tax Information, see Note 1, below.</p>

breaches of access security; Virus infections	
Incidents which may involve significant employee misconduct, including serious violation of policy or theft.	Your manager and Human Resources.
Loss of public funds, assets, and illegal activity	Operations Review and Consultation, as prescribed by DSHS Administrative Policy 16.10 Reporting Known or Suspected Loss of Public Funds or Assets to the State Auditor's Office
Welfare or vendor fraud	DSHS Office of Fraud and Accountability at 360-664-5505 or Welfare Fraud Hotline at 1-800-562-6906

Note 1: Federal Tax Information (FTI): Upon discovery of a possible improper inspection or disclosure of FTI, the individual making the observation or receiving information must, besides reporting the incident as described above, directly contact the Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), Denver Office, at 303-446-1880 (or 800-366-4484 or 510-637-2558) (see also <http://www.treasury.gov/tigta/>).

The DSHS IT Security Administrator will:

- Notify the DSHS Privacy Officer in cases where confidential information may have been compromised and assist in conducting a risk assessment of the breach and in developing mitigation efforts. If a breach is established, work with the DSHS Privacy Officer to follow requirements of applicable state and federal laws, including the HIPAA Privacy and Security Rules.
- Report incidents in accordance with the WACIRC incident reporting process.
- Upon notification of a potential loss, theft, or unauthorized disclosure of Federal Tax Information (FTI), immediately ensure that the Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards, are notified.

NOTE: See additional requirements for reporting incidents at [Administrative Policy 9.01 Incident Reporting](#).

Section P10.2.2.S2 was renumbered to become P10.2.2.S1 (Revision 13; 2012).

Section P10.2.2.S4 was eliminated from this manual (Revision 10; 2009). Information on securing and protecting evidence was moved to sections P10.2.4.S2 through P10.2.4.S7).

Section P10.2.3.S2 was eliminated, and its contents moved to P5.2.9.G1 (Revision 11).

P10.2.3.S3 ACCESSING EMPLOYEES' FILES

Supervisors may obtain access to messages and files residing on department systems as follows:

1. By requesting access from the system user who has primary control over the message or file.
2. If the system user is unavailable, and the information is necessary to conduct required business functions, the user's manager will:
 - a. Submit a written request for access, to the appropriate IT staff; and
 - b. Notify the user in writing, within 24 hours of each occurrence of the access. The notification must provide a reasonable justification for the access.
3. If either of the above steps would delay or interfere with an investigation or compliance with a public records or discovery request, request authorization from the user's appointing authority.

NOTE: For investigations initiated by appointing authority, see [DSHS IT Security Policy Manual section 10.2.4 Investigations](#).

Section P10.2.3.S4 was renumbered to become P10.2.3.S3 (Revision 13; 2012).

P10.2.4.S2 PROTECTING CONFIDENTIALITY DURING AN INVESTIGATION

Investigations are sensitive by their nature. It is important to maintain confidentiality to the degree possible while supporting investigations. For this reason:

1. The number of staff engaged in or made aware of the investigation should be kept to the minimum necessary to conduct the investigation.
2. Staff with knowledge of the investigation should be reminded of their responsibility to keep investigatory information confidential.
3. Collection of data in support of investigations, such as accessing the subject's files from their machine, or acquiring a forensic copy of their hard drive, should be done after hours and/or out of view of co-workers.

P10.2.4.S3 THE TWO PERSON RULE

The two person rule is intended to ensure and document the integrity of the data gathering process. This protects both the agency and the individuals who gather the data. The data gathering process must be conducted by two people until the data

has been preserved in a verifiable, unalterable form, such as a read only optical disc (CD/DVD with the session closed) that is signed by both participants. One person will gather the data, and another will verify and record the steps taken. This documents that the data was gathered correctly, is valid, and that no data was created, destroyed, or altered during the collection process. See [Sample Data Collection Log form](#) which can be used as a template.

Care must be taken to ensure that the data collection techniques will stand up under scrutiny. Such collection should always be done with the expectation that the material will end up in court.

P10.2.4.S4 CHAIN OF CUSTODY

Chain of custody requires that from the moment data is collected, every transfer of that data from person to person, or place to place be documented, *and* that when stored, it is stored securely, and not accessed without authorization. This requires:

1. That the person(s) collecting the data, document and sign for initial possession.
2. That everyone who relinquishes or takes custody of the data acknowledge the transfer by signature.
3. That, when in transit, media containing the data is never left unattended or with an unauthorized person.
4. Storing the data in such a way that only authorized persons have access to it, and documenting their access to it.

See [sample Chain of Custody form](#), which can be used as a template.

P10.2.4.S5 SUSPECTED CRIMINAL ACTIVITY

If evidence of criminal activity is found, data collection will cease, and the appointing authority or manager leading the investigation must be notified immediately. Management will make the determination as to whether or not the data indicates criminal activity, and, if so, will notify DSHS Human Resources Division (HRD) and the DSHS IT Security Administrator.

P10.2.4.S7 IT SUPPORT FOR INVESTIGATIONS

After being assigned the task of data collection for an investigation, the following steps should be taken:

A. Information Sharing

The IT staff supporting the investigation, or a representative thereof, should confer with a manager who has a clear understanding of the suspected policy violation being investigated. This provides an opportunity to discuss the data to be collected, and how and when that collection will take place.

B. Preparation for Data Collection

The collection of data for an investigation requires knowing beforehand:

1. What data will be collected.
2. Where that data resides.
3. Who will be assigned to do the data collection. Important – All aspects of the data collection process must have two (or more) people working together.
4. How the data will be obtained. Bear in mind that the data collection must be documented, and done discretely.
5. Where the data will be stored. This must be a secure location to prevent compromising the investigation or the confidentiality thereof.

C. Collecting Data

See [P10.2.4.S3 The Two Person Rule](#), [P10.2.4.S4 Chain of Custody](#), and [P10.2.4.S5 Suspected Criminal Activity](#) prior to collecting evidence.

The nature of the suspected policy violation will often determine where desired data is likely to reside. The investigator will need to communicate effectively with the IT staff involved in the investigation to ensure complete and timely collection of the data. Likely sources of this data include:

- Internet history, downloaded files, .PSTs, etc from the subject computer(s). Ideally, files should be written to another medium which can be examined later. The two person rule should be followed when gathering or handling the data, until such time as it has been written to a read-only medium. Opening the original copy of the file on the hard drive or on a write-many medium will change file dates and hurt the evidentiary value.
- The subject's Exchange mailbox. The contents of the mailbox should be written to a read-only medium.

- Collection of files in the subject's home network folder, and in any folders to which the subject has access. Care should be taken to limit the collection to those files which the subject has control or authorship of.
- Windows System and/or Security logs, or syslogs from infrastructure equipment (e.g. routers, switches).

D. Final Data Collection Report

The final report to management may be written or verbal. The content and format of the report may vary, but there are two types of documentation that must be maintained:

- Data collection notes, documenting the steps taken and witnessed, to verify the integrity of the collection process; and
- Chain of custody information for any data gathered.

E. Forensic Examination of Media

The appointing authority may, in consultation with Human Resources, decide to have a forensic examination conducted on the original media from which the investigatory data was collected, or in lieu of that collection. In these cases, the original media from which the data is desired will be provided to a qualified forensic examiner for acquisition and analysis of the data on that media.

Computer forensics is the collection, examination, and analysis of digital information. A forensic investigation requires that the data collected be *identical* to that found on the original media. The forensically sound collection of data requires specialized tools, techniques and training, and should not be performed by staff that lack either the tools or the training. Prior to beginning the process of forensic data collection, consultation with the DSHS IT Security Administrator is required.

Acceptable forensic examiners for DSHS are:

1. State Auditors Office.
2. Washington State Patrol.
3. Private industry vendors of computer forensic services.
4. DSHS staff who have been approved by the DSHS IT Security Administrator to perform forensic examinations. That approval requires that the administration seeking to perform in-house forensic examinations meets the following criteria:

- a. Has written procedures for conducting forensically sound investigations that would stand up to scrutiny in court;
- b. Possesses the tools required to perform a forensically sound investigation;
- c. Has staff trained in the use of those tools, and who have demonstrated proficiency with them; and
- d. Has a secure facility for the storage of evidence collected, and in which to conduct forensic acquisition and analysis.

Once a forensic examination is completed, a report is produced detailing the results of the analysis of that examination, for the use of management in determining the final disposition of the investigation.

Chapter 11: Safeguarding Federal Information

This chapter contains:

- [P11.3.2.S8 DESTRUCTION OF DOCUMENTS CONTAINING IRS TAX INFORMATION](#)
- [P11.4.1.S4 PROCESSING "HIT" INFORMATION BY QA FIELD OFFICE](#)

P11.3.2.S8 DESTRUCTION OF DOCUMENTS CONTAINING IRS TAX INFORMATION

IRS Publication 1075, Section 8.0, covers the disposal of IRS tax information.

- A. Both the Economic Services Administration, Operations Support Division (ESA-OSD), Quality Assurance (QA); and the Division of Child Support (DCS); shall destroy reports or screen prints containing IRS tax information when they are no longer needed. At the time of destruction, the date of destruction and the name of the person performing the destruction are entered on the report control log(s). The report logs are maintained for five years after the date of the last entry.
- B. QA and DCS shall destroy documents containing IRS tax information by shredding, pulping, or incinerating. When shredding, the paper should be inserted so that lines of print are perpendicular to the cutting line. The paper should be shredded to a width of 5/16 inch or smaller strips. A DSHS employee shall witness the destruction.
- C. QA and DCS shall furnish the DSHS IT Security Administrator a certificate of destruction covering documents destroyed each year. The information should identify the material destroyed and the date and manner of destruction.
- D. This information is a required element of the annual safeguard activity report and is due to the DSHS IT Security Administrator on or before August 15 of each year for QA, and February 15 for DCS.

Section P11.4.1 S4 Processing "HIT" Information by QA Field Office, was eliminated from this manual (Revision 14.2, 2015).

Section P12.4 MAPPER Applications Security, was eliminated from this manual (Revision 9, March 2008).