Effective Information Systems Security Officer (ISSO) Training

2013 Joint Security Awareness
Council Seminar

Kathy Clark

8-104. Information System Security Officer(s) (ISSO). ISSOs may be appointed by the ISSM in facilities with multiple accredited IS. The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

a. Ensure the implementation of security measures, in accordance with facility procedures.

b. Identify and document any unique threats.

c. If so directed by the GCA and/or if an identified unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in this chapter are required.

d. Develop and implement a certification test as required by the ISSM/CSA.

e. Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions.

f. Notify the CSA (through the ISSM) when an IS no longer processes classified information, or when changes occur that might affect accreditation.

g. Ensure:

(1) That each IS is covered by the facility Configuration Management Program, as applicable.

(2) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

(3) That unauthorized personnel are not granted use of, or access to, an IS.

(4) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

h. Document any special security requirement identified by the GCA and the protection measures implemented to fulfill these requirements for the information contained in the IS.

i. Implement facility procedures:

(1) To govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(3) For the reporting of IS security incidents and initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

(4) Requiring that each IS user sign an acknowledgment of responsibility for the security of IS and classified information.

(5) For implementing and maintaining security-related software for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

j. Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

k. Evaluate proposed changes or additions to the IS, and advises the ISSM of their security relevance.

l. Ensure that all active user Ids are revalidated at least annually.

TECHNICAL SECURITY

Computer Systems Security Analysts (CSSA)

INFORMATION TECHNOLOGY

Closed Area Support Team (CAS Team)

PROGRAM ENGINEERS

Program Engineers

ASSIGNED RESPONSIBILITIES:

- Ensure that unauthorized personnel are not granted use of, or access to an IS.

- Ensure that system recovery processes are monitored to ensure that security features and procedures are properly restored.

- Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

- Evaluate proposed changes or additions to the IS (including hardware, software or connectivity, and advise the ISSM of their security relevance.

- Verify that prior to being granted access to an IS, user clearances and accesses are verified and the user is trained on there is responsibilities. (i.e., IS Access Authorization and Briefing Form has been completed)

- Ensure that all active user IDs are revalidated at least annually.

- Perform IS weekly audit reviews.

- Initial Training from ISSM
- CSSA meets with ISSO
    - Sign ISSO Delegation Record
    - Distribute ISSO Task Checklist
    - Distribute Link to Dallas ISSO Sharepoint
    - Distribute the Weekly Audit Record
    - Distribute ISSO Quick Reference Guide
    - Monthly Meetings between the CSSA and ISSO
    - Quarterly ISSO Meetings – All Facility ISSOs

ISSO Responsibilities

- ISSO duties and responsibilities as outlined in the National Industrial Security Program Operating Manual and Industrial Security Field Operating Manual
  - Ensure that unauthorized personnel are not granted use of, or access to a system.
  - Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.
  - Notify ISSM of any proposed changes and wait for approval.
  - Train and brief users on appropriate IS use and procedures.
  - Notify ISSM of any changes to duty assignment.
  - Ensure systems are decertified according to approved procedures.

Who Should Be Notified When?

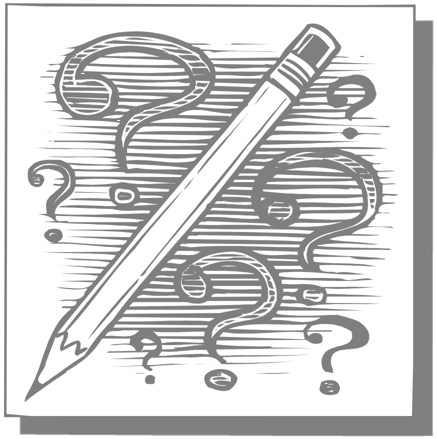
- Equipment not functioning
  - ISSO & ISSM
- Equipment requiring sanitizing
  - ISSO & ISSM
- Suspicious use of the systems (usually associated with Need-To-Know)
  - ISSO & ISSM
- Visitors not being escorted
  - ISSO & ISSM
- When someone no longer needs access to the system

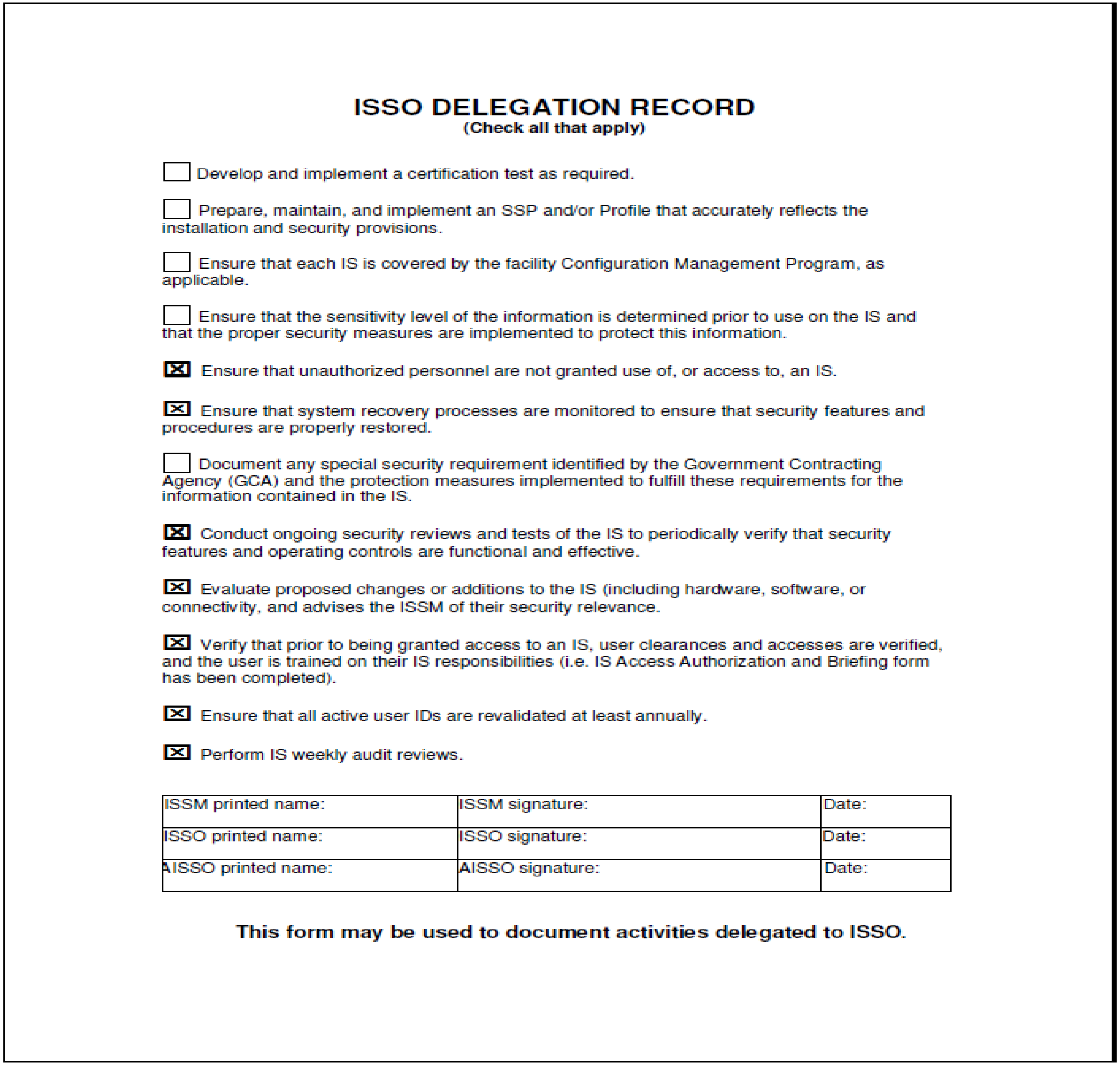
Train and brief users on IS use and procedures.

- As the ISSO you are responsible for training users on the policies and procedures for classified processing. This includes:
  - Processing Procedures
  - Marking Requirements
  - Unattended Processing
  - Password Creation
  - Restricted or Closed Area Requirements
    - Many problems associated with use can be solved by reading the Protection Profile. It is acceptable, and even preferred, for the user to follow step by step instructions by reading from the Protection Profile.

Audit Records

- Who fills out what?
  - ISSOs & Users
- What logs are required? - <u>Manual</u>
  - Maintenance
    - Hardware & Software
  - Upgrade/Downgrade
  - Sanitization
  - Weekly Audit Log
    - Custodian
  - Seal Log (If Applicable)





ISSO DELEGATION RECORD

(Check all that apply)

□ Develop and implement a certification test as required.

□ Prepare, maintain, and implement an SSP and/or Profile that accurately reflects the installation and security provisions.

□ Ensure that each IS is covered by the facility Configuration Management Program, as applicable.

□ Ensure that the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

☒ Ensure that unauthorized personnel are not granted use of, or access to, an IS.

☒ Ensure that system recovery processes are monitored to ensure that security features and procedures are properly restored.

□ Document any special security requirement identified by the Government Contracting Agency (GCA) and the protection measures implemented to fulfill these requirements for the information contained in the IS.

☒ Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

☒ Evaluate proposed changes or additions to the IS (including hardware, software, or connectivity, and advises the ISSM of their security relevance.

☒ Verify that prior to being granted access to an IS, user clearances and accesses are verified, and the user is trained on their IS responsibilities (i.e. IS Access Authorization and Briefing form has been completed).

☒ Ensure that all active user IDs are revalidated at least annually.

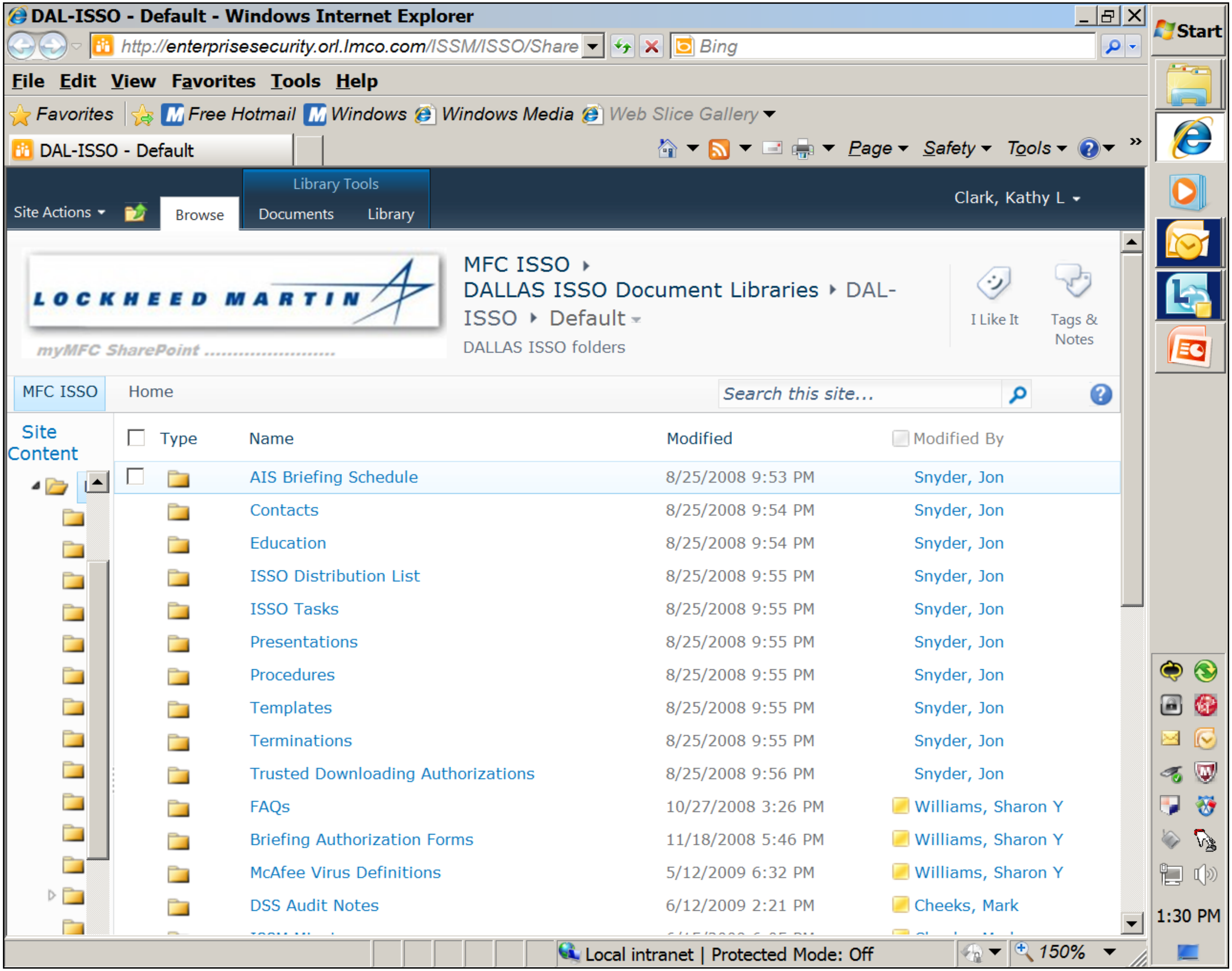
☒ Perform IS weekly audit reviews.

ISSM printed name:	ISSM signature:	Date:
ISSO printed name:	ISSO signature:	Date:
AISSO printed name:	AISSO signature:	Date:

This form may be used to document activities delegated to ISSO.

MFC DEVELOPED ISSO TOOLS FOR TRAINING

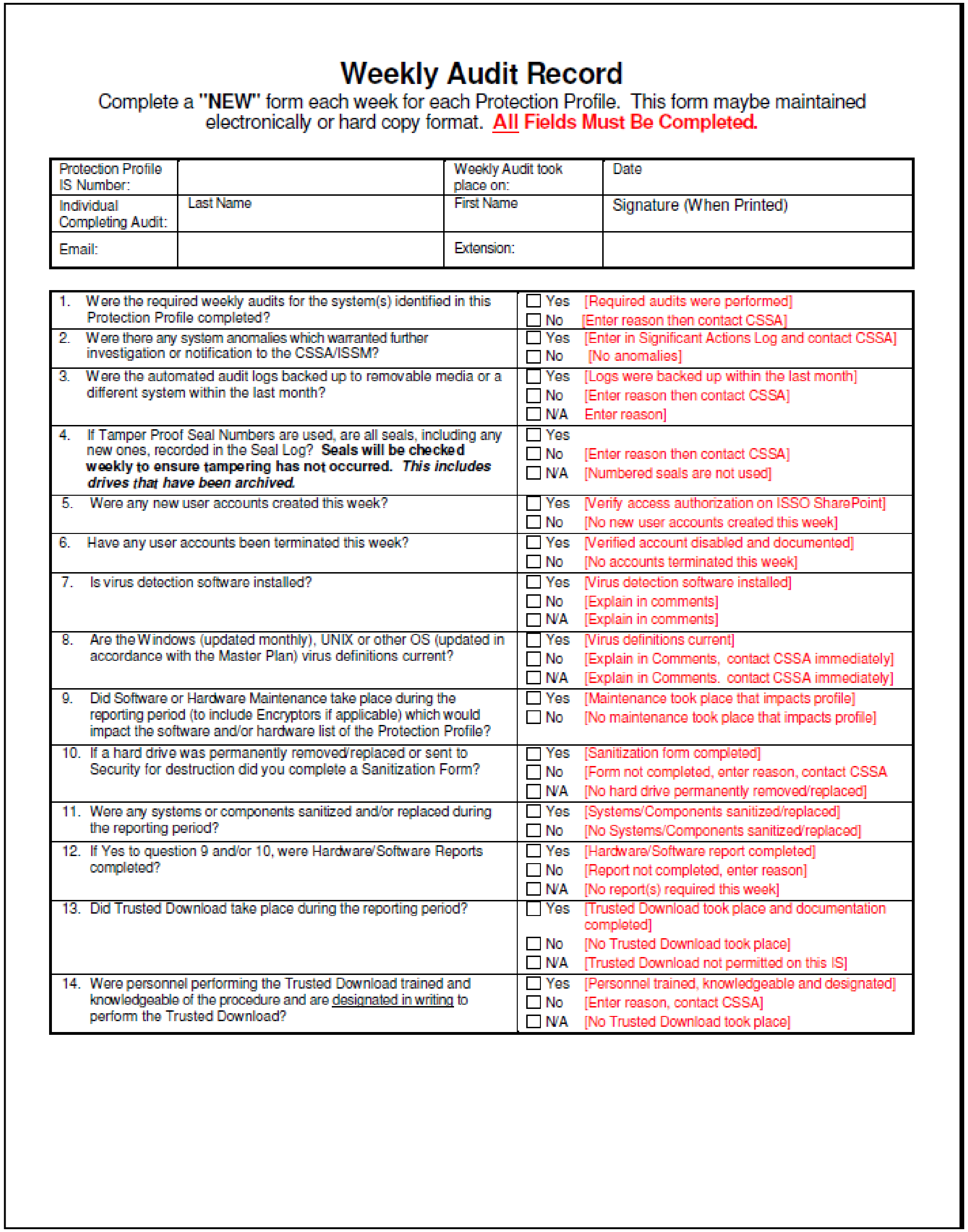
Information System Security Officer Tasks
Tasks listed herein may be performed by the Information System Security Officer (ISSO), Computer System Security Analyst (CSSA) or System Administrator (SA).
Special Access Program (SAP) ISSOs, CSSAs, and SAs must coordinate with the Contractor Program Security Officer (CPSO) for program specific requirements regarding media storage, labeling and destruction requirements. Also refer to each SAP System Security Plan (SSP) for update frequency of anti-virus definition files
Daily
□ Perform random visual inspection of Protected Distribution System (PDS)
□ Review area for unmarked media. If found secure and label in accordance with program directives. **(Reference "Template" folder on ISSO Share Point for collateral programs label format. SAP label formats available via the CPSO).**
Weekly
□ Review and/or run Audit logs
□ Review SSP Reports and Logs (i.e. Hardware Reports, Software Reports, Maintenance Logs, Sanitization Forms and Seal Logs)
□ Review ISSO Share Point for new information
□ CompleteWeekly Audit Record form
Monthly
□ Perform Backup of Audit History. Maintain 1 Inspection Cycle of history records. Destroy older records in accordance with media destruction procedures.
□ Update Anti-Virus Definition files
□ Review and complete encryptor audit log
Quarterly
□ Attend ISSO briefings
Annually
□ Revalidate user accounts and access
□ Remove logs more than 1 Inspection Cycle
□ Perform technical inspection of PDS



MFC ISSO ▸ DALLAS ISSO Document Libraries ▸ DAL-ISSO ▸ Default

DALLAS ISSO folders

Type	Name	Modified	Modified By
	AIS Briefing Schedule	8/25/2008 9:53 PM	Snyder, Jon
	Contacts	8/25/2008 9:54 PM	Snyder, Jon
	Education	8/25/2008 9:54 PM	Snyder, Jon
	ISSO Distribution List	8/25/2008 9:55 PM	Snyder, Jon
	ISSO Tasks	8/25/2008 9:55 PM	Snyder, Jon
	Presentations	8/25/2008 9:55 PM	Snyder, Jon
	Procedures	8/25/2008 9:55 PM	Snyder, Jon
	Templates	8/25/2008 9:55 PM	Snyder, Jon
	Terminations	8/25/2008 9:55 PM	Snyder, Jon
	Trusted Downloading Authorizations	8/25/2008 9:56 PM	Snyder, Jon
	FAQs	10/27/2008 3:26 PM	Williams, Sharon Y
	Briefing Authorization Forms	11/18/2008 5:46 PM	Williams, Sharon Y
	McAfee Virus Definitions	5/12/2009 6:32 PM	Williams, Sharon Y
	DSS Audit Notes	6/12/2009 2:21 PM	Cheeks, Mark



Weekly Audit Record

Complete a "**NEW**" form each week for each Protection Profile. This form maybe maintained electronically or hard copy format. **All Fields Must Be Completed.**

Protection Profile IS Number:		Weekly Audit took place on:	Date
Individual Completing Audit:	Last Name	First Name	Signature (When Printed)
Email:		Extension:	

1. Were the required weekly audits for the system(s) identified in this Protection Profile completed?	☐ Yes [Required audits were performed] ☐ No [Enter reason then contact CSSA]
2. Were there any system anomalies which warranted further investigation or notification to the CSSA/ISSM?	☐ Yes [Enter in Significant Actions Log and contact CSSA] ☐ No [No anomalies]
3. Were the automated audit logs backed up to removable media or a different system within the last month?	☐ Yes [Logs were backed up within the last month] ☐ No [Enter reason then contact CSSA] ☐ N/A Enter reason]
4. If Tamper Proof Seal Numbers are used, are all seals, including any new ones, recorded in the Seal Log? **Seals will be checked weekly to ensure tampering has not occurred.** ***This includes drives that have been archived.***	☐ Yes ☐ No [Enter reason then contact CSSA] ☐ N/A [Numbered seals are not used]
5. Were any new user accounts created this week?	☐ Yes [Verify access authorization on ISSO SharePoint] ☐ No [No new user accounts created this week]
6. Have any user accounts been terminated this week?	☐ Yes [Verified account disabled and documented] ☐ No [No accounts terminated this week]
7. Is virus detection software installed?	☐ Yes [Virus detection software installed] ☐ No [Explain in comments] ☐ N/A [Explain in comments]
8. Are the Windows (updated monthly), UNIX or other OS (updated in accordance with the Master Plan) virus definitions current?	☐ Yes [Virus definitions current] ☐ No [Explain in Comments, contact CSSA immediately] ☐ N/A [Explain in Comments. contact CSSA immediately]
9. Did Software or Hardware Maintenance take place during the reporting period (to include Encryptors if applicable) which would impact the software and/or hardware list of the Protection Profile?	☐ Yes [Maintenance took place that impacts profile] ☐ No [No maintenance took place that impacts profile]
10. If a hard drive was permanently removed/replaced or sent to Security for destruction did you complete a Sanitization Form?	☐ Yes [Sanitization form completed] ☐ No [Form not completed, enter reason, contact CSSA ☐ N/A [No hard drive permanently removed/replaced]
11. Were any systems or components sanitized and/or replaced during the reporting period?	☐ Yes [Systems/Components sanitized/replaced] ☐ No [No Systems/Components sanitized/replaced]
12. If Yes to question 9 and/or 10, were Hardware/Software Reports completed?	☐ Yes [Hardware/Software report completed] ☐ No [Report not completed, enter reason] ☐ N/A [No report(s) required this week]
13. Did Trusted Download take place during the reporting period?	☐ Yes [Trusted Download took place and documentation completed] ☐ No [No Trusted Download took place] ☐ N/A [Trusted Download not permitted on this IS]
14. Were personnel performing the Trusted Download trained and knowledgeable of the procedure and are designated in writing to perform the Trusted Download?	☐ Yes [Personnel trained, knowledgeable and designated] ☐ No [Enter reason, contact CSSA] ☐ N/A [No Trusted Download took place]

Reasons/Comments

As required above, enter reasons or comments in this section. Begin with the question number followed by the explanation, if maintaining by hardcopy, circle the question number; if maintaining electronically, and enclose question number with parenthesis, e.g. (1).

Failure to comply with the Master System Security Plan, Protection Profile, NISPOM or the Company Security Manual can result in an Infraction, Security Violation, Suspension of Access, or Decertification of the Accredited Computer System(s). By submitting this weekly audit record I certify the information contained herein is correct.

Weekly Record Audit

Auditing involves recognizing, recording, storing and analyzing information related to security-relevant activities. All on-line Audits must be backed up either to Tape, CD, DVD, External Drive, Hardcopy etc., at least once a month.

Virus Detection

All PCs and UNIX/LINUX systems must have Virus detection software installed. All files must be checked for viruses and malicious code before being introduced on an IS. IRIX and other legacy computers not supported by antivirus products shall be identified in the Protection Profile how files are scanned for viruses and malicious code prior to use.

Maintenance Action

All maintenance actions (Software and Hardware) shall be recorded in enough detail to reflect actual events (i.e. describe maintenance action, nomenclature or system/device description, unique identifier, serial number and or personnel etc.). Sanitization of components shall correspond to the DSS Clearing and Sanitization Matrix or specialized procedures identified in the Protection Profile. Sanitization by overwriting hard drives is NOT approved. Classified hard drives shall be returned to the appropriate security office and destroyed by prescribed methods or cleared and reused at the same or higher classification level.

Unless otherwise directed by the ISSM, memory shall be cleared in accordance with the DSS Clearing and Sanitization Matrix by one of the following methods:

- Remove of all power including battery power
- Overwrite all addressable locations with a single character
- Perform a full chip erase as per manufacturer's data sheets
- Perform an ultraviolet erase according to manufacturer's recommendation according to Memory type

Trusted Downloads

Trusted Downloads are limited to only the file formats identified in the DSS Approved procedure.

Marking Classified Material

All classified material must have cover sheets (front and back), as well as the following required markings:

- Overall classification
- Title or subject
- Origination Date
- Declassify On
- Identity of Originating Agency (i.e. Lockheed Martin Missiles and Fire Control, PO Box 650003, Dallas, TX 75265)

But wait……….can it get any better???? Well, YES IT CAN!!!!

LOCKHEED MARTIN

MISSILES AND FIRE CONTROL

Information Systems Security Officer
Quick Reference Guide

Mission Statement

Provide world class technical security to our customers domestic and abroad. Continually offer meaningful and relevant training to our Information Systems Security Officers, and remain dedicated to the protection of the war fighter by maintaining the confidentiality, integrity, and availability of our classified systems and networks.

Key Personnel

- Information Systems Security Manager (ISSM)

  XXXXX x 3-XXXX

- Computer Systems Security Analyst (CSSA)

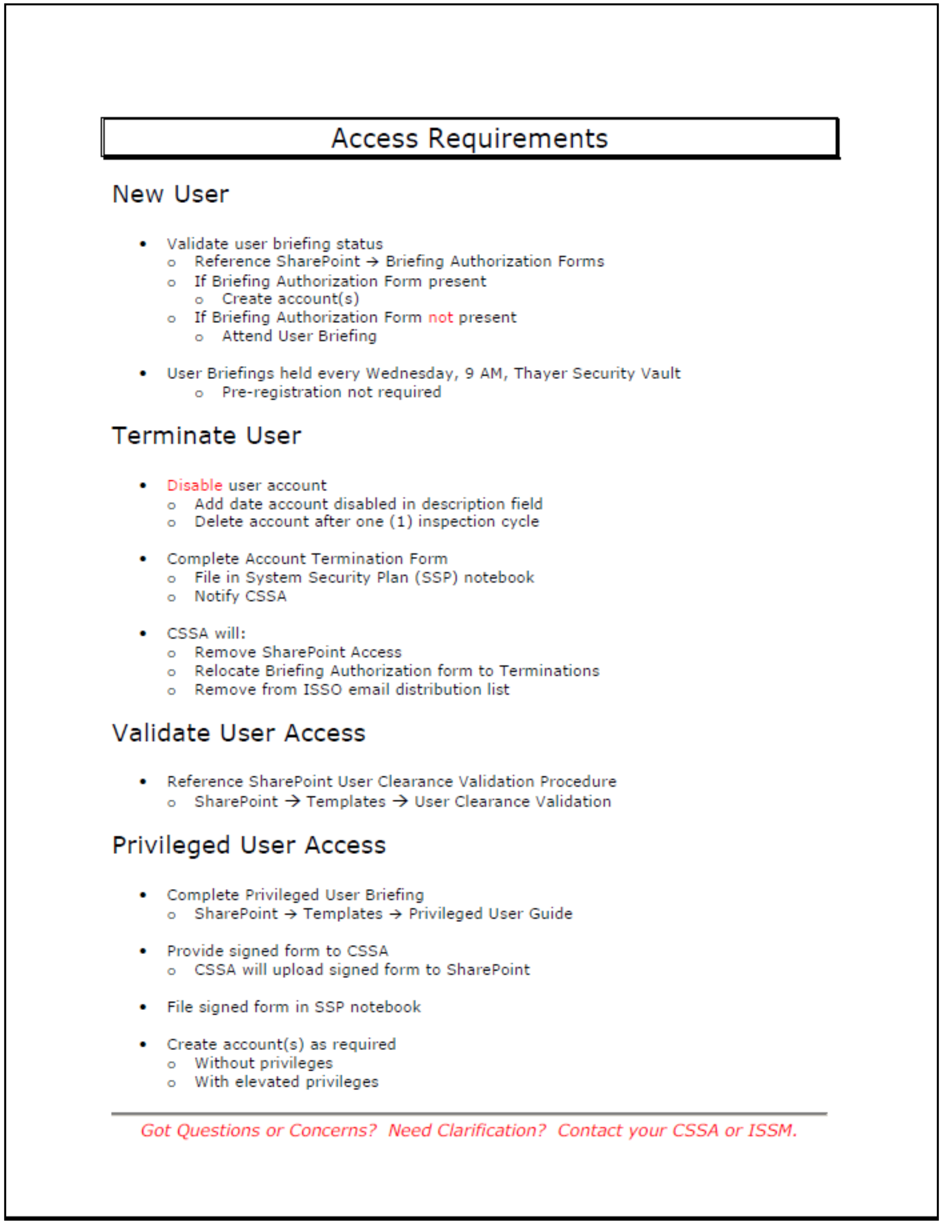
  XXXXX x 3-XXXX

- Alternate CSSA

  XXXXX x 3-XXXX

- Systems Administrator

  XXXXX x 3-XXXX



Access Requirements

New User

- Validate user briefing status
  - Reference SharePoint → Briefing Authorization Forms
  - If Briefing Authorization Form present
    - Create account(s)
  - If Briefing Authorization Form not present
    - Attend User Briefing

- User Briefings held every Wednesday, 9 AM, Thayer Security Vault
    - Pre-registration not required

Terminate User

- Disable user account
  - Add date account disabled in description field
  - Delete account after one (1) inspection cycle

- Complete Account Termination Form
  - File in System Security Plan (SSP) notebook
  - Notify CSSA

- CSSA will:
  - Remove SharePoint Access
  - Relocate Briefing Authorization form to Terminations
  - Remove from ISSO email distribution list

Validate User Access

- Reference SharePoint User Clearance Validation Procedure
  - SharePoint → Templates → User Clearance Validation

Privileged User Access

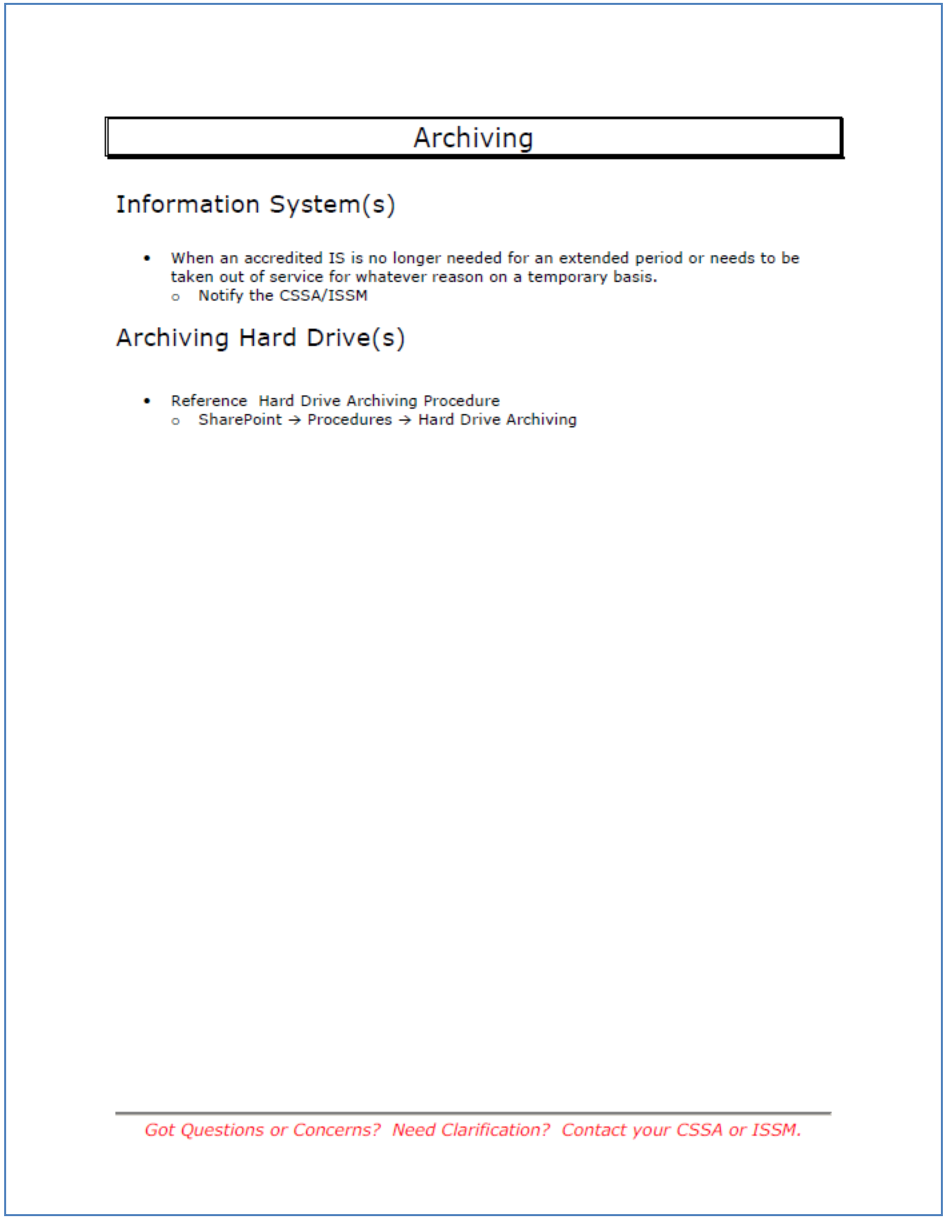
- Complete Privileged User Briefing
  - SharePoint → Templates → Privileged User Guide

- Provide signed form to CSSA
  - CSSA will upload signed form to SharePoint

- File signed form in SSP notebook

- Create account(s) as required
  - Without privileges
  - With elevated privileges

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Archiving

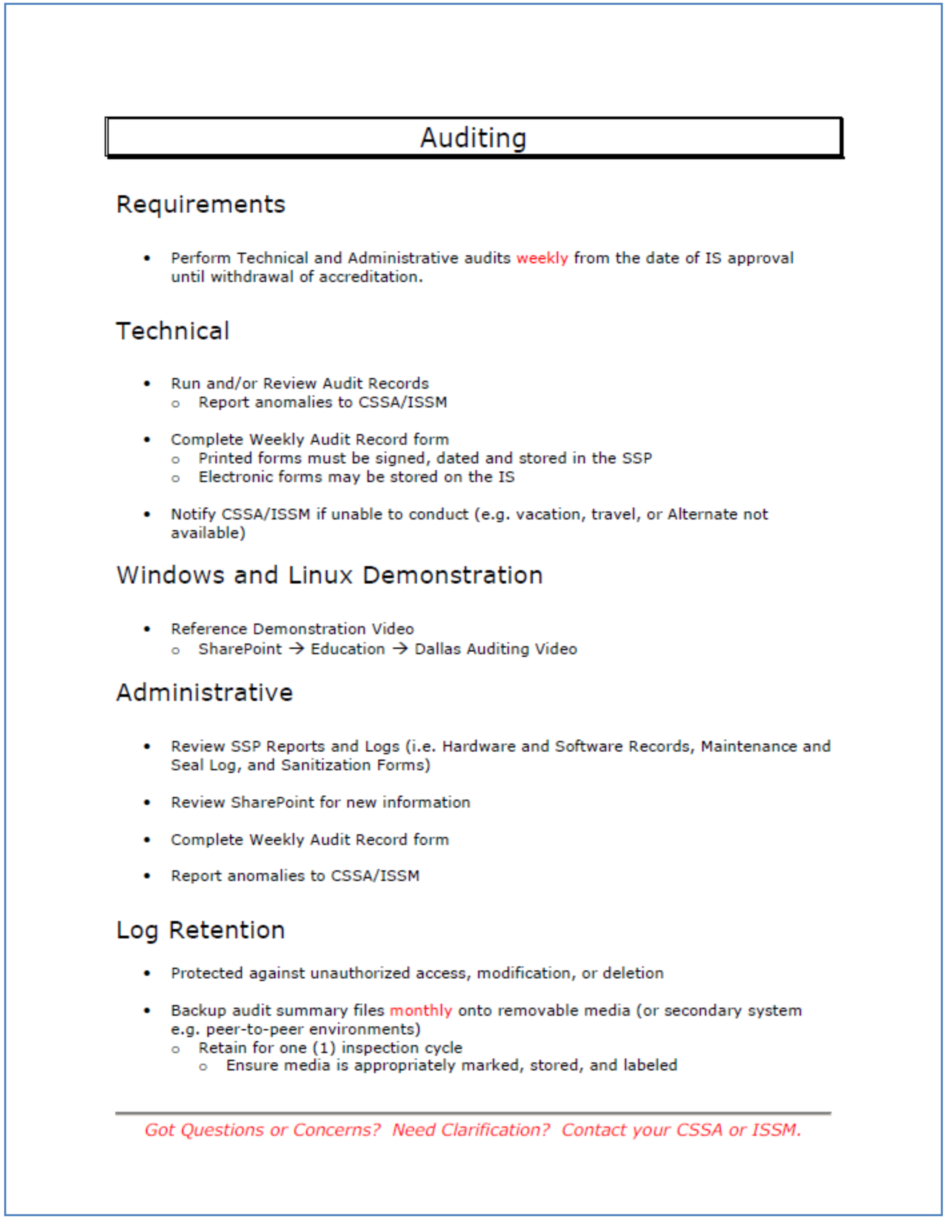
Information System(s)

- When an accredited IS is no longer needed for an extended period or needs to be taken out of service for whatever reason on a temporary basis.
    - Notify the CSSA/ISSM

Archiving Hard Drive(s)

- Reference Hard Drive Archiving Procedure
    - SharePoint → Procedures → Hard Drive Archiving

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Auditing

Requirements

- Perform Technical and Administrative audits weekly from the date of IS approval until withdrawal of accreditation.

Technical

- Run and/or Review Audit Records
  - Report anomalies to CSSA/ISSM
- Complete Weekly Audit Record form
  - Printed forms must be signed, dated and stored in the SSP
  - Electronic forms may be stored on the IS
- Notify CSSA/ISSM if unable to conduct (e.g. vacation, travel, or Alternate not available)

Windows and Linux Demonstration

- Reference Demonstration Video
  - SharePoint → Education → Dallas Auditing Video

Administrative

- Review SSP Reports and Logs (i.e. Hardware and Software Records, Maintenance and Seal Log, and Sanitization Forms)
- Review SharePoint for new information
- Complete Weekly Audit Record form
- Report anomalies to CSSA/ISSM

Log Retention

- Protected against unauthorized access, modification, or deletion
- Backup audit summary files monthly onto removable media (or secondary system e.g. peer-to-peer environments)
  - Retain for one (1) inspection cycle
    - Ensure media is appropriately marked, stored, and labeled

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.

Backups

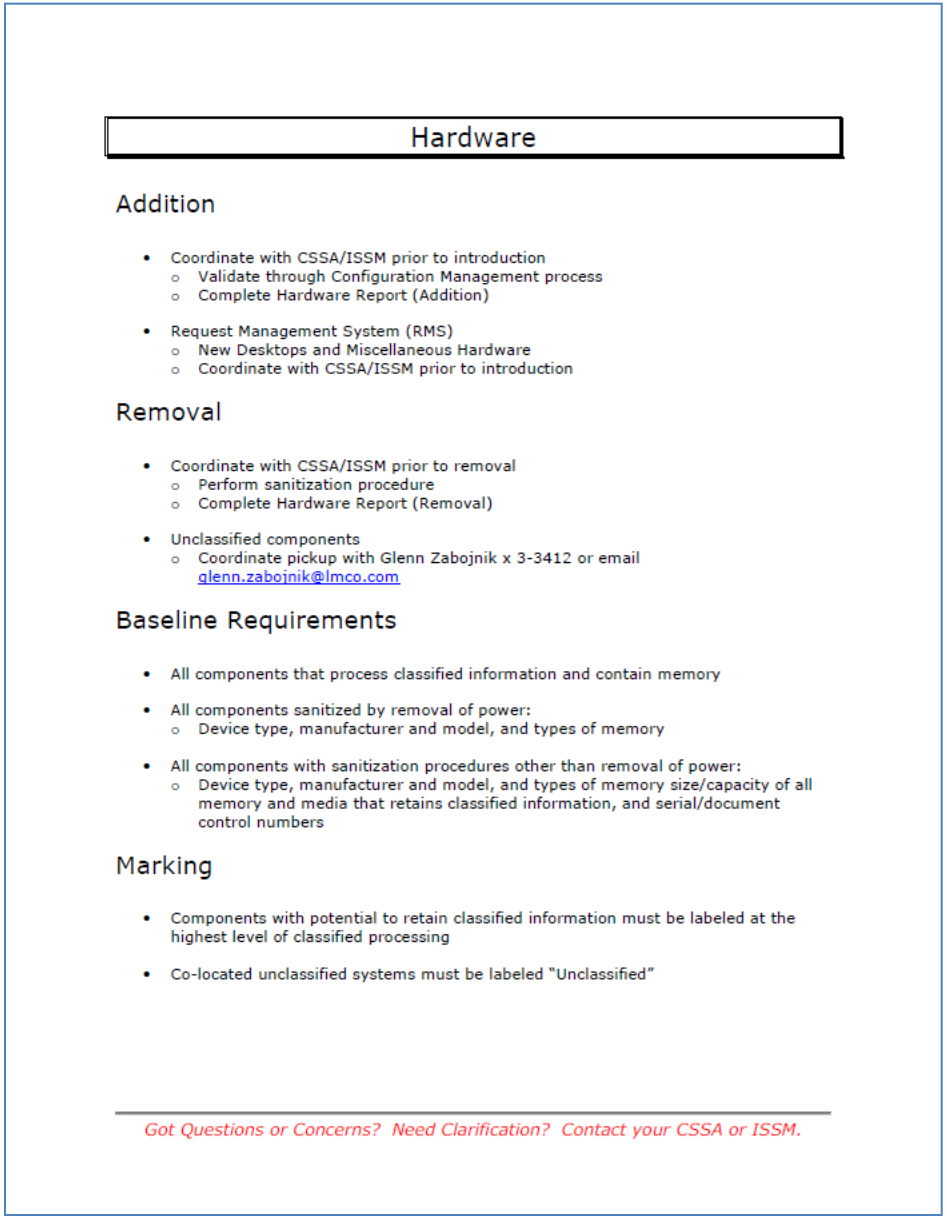
Backup Requirements and strategies vary from program to program based upon requirements located in the DD-254 and other Program Directives. For the purpose of the ISSO Quick Reference Guide "Backups" are limited to audit history data.

- Backup audit summary files monthly onto removable media (or secondary system e.g. peer-to-peer environments)
  - External devices (e.g. USB drives, CDRs, DVRs)
    - Add device to Hardware Baseline
    - Complete Maintenance, Operating System & Security Software Change Log on each use

- Retain one (1) inspection cycle worth of audit summary files

- Ensure media/device is appropriately marked, stored, and labeled

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Hardware

Addition

- Coordinate with CSSA/ISSM prior to introduction
  - Validate through Configuration Management process
  - Complete Hardware Report (Addition)
- Request Management System (RMS)
  - New Desktops and Miscellaneous Hardware
  - Coordinate with CSSA/ISSM prior to introduction

Removal

- Coordinate with CSSA/ISSM prior to removal
  - Perform sanitization procedure
  - Complete Hardware Report (Removal)
- Unclassified components
  - Coordinate pickup with Glenn Zabojnik x 3-3412 or email glenn.zabojnik@lmco.com

Baseline Requirements

- All components that process classified information and contain memory
- All components sanitized by removal of power:
  - Device type, manufacturer and model, and types of memory
- All components with sanitization procedures other than removal of power:
  - Device type, manufacturer and model, and types of memory size/capacity of all memory and media that retains classified information, and serial/document control numbers

Marking

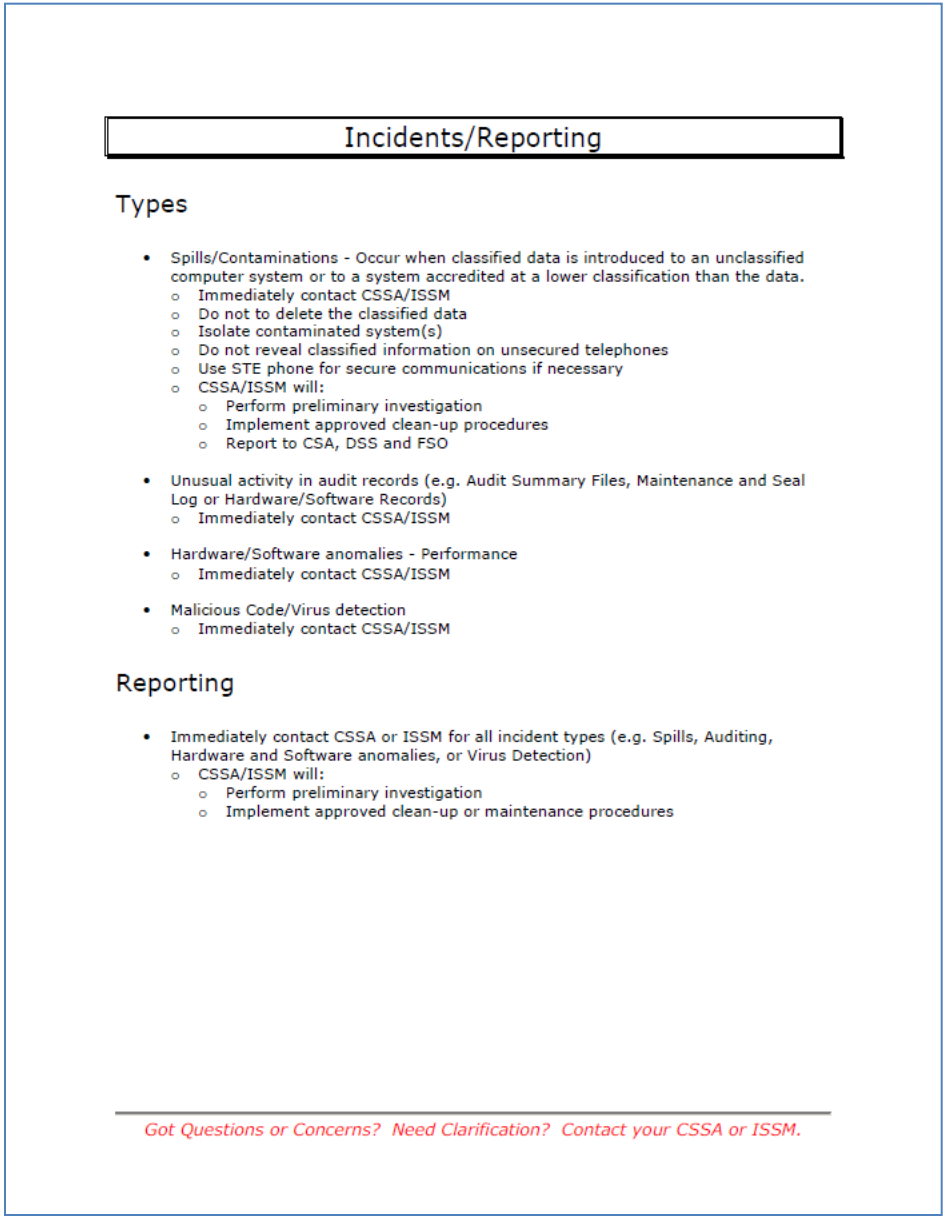
- Components with potential to retain classified information must be labeled at the highest level of classified processing
- Co-located unclassified systems must be labeled "Unclassified"

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.

Hardware (Continued)

External Devices (e.g. USB drives, CDRs, DVRs)

- Add to Hardware Baseline
- Mark, store, and label appropriately
- Complete Maintenance, Operating System& Security Software Change Log on each use



Incidents/Reporting

Types

- Spills/Contaminations - Occur when classified data is introduced to an unclassified computer system or to a system accredited at a lower classification than the data.
  - Immediately contact CSSA/ISSM
  - Do not to delete the classified data
  - Isolate contaminated system(s)
  - Do not reveal classified information on unsecured telephones
  - Use STE phone for secure communications if necessary
  - CSSA/ISSM will:
    - Perform preliminary investigation
    - Implement approved clean-up procedures
    - Report to CSA, DSS and FSO

- Unusual activity in audit records (e.g. Audit Summary Files, Maintenance and Seal Log or Hardware/Software Records)
  - Immediately contact CSSA/ISSM

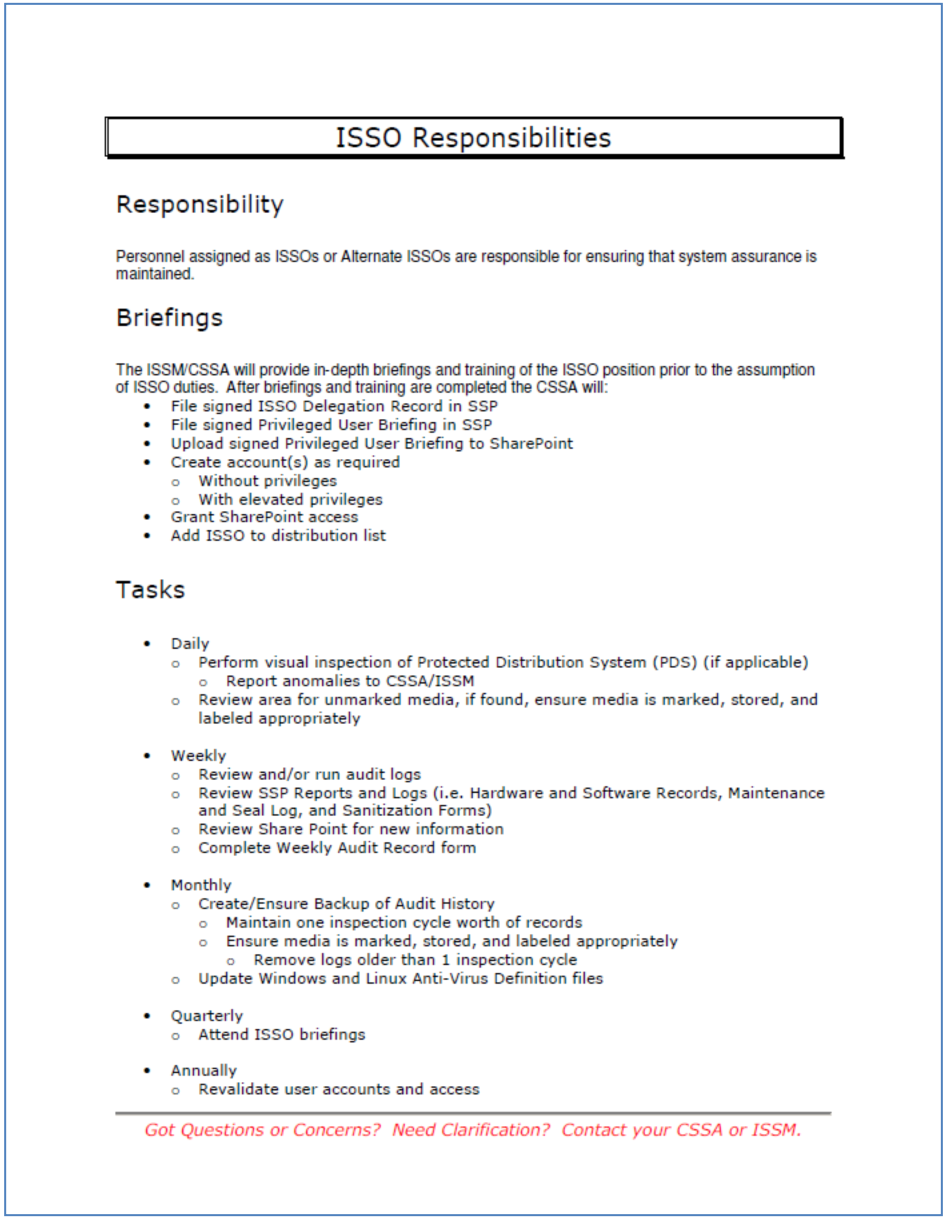
- Hardware/Software anomalies - Performance
  - Immediately contact CSSA/ISSM

- Malicious Code/Virus detection
  - Immediately contact CSSA/ISSM

Reporting

- Immediately contact CSSA or ISSM for all incident types (e.g. Spills, Auditing, Hardware and Software anomalies, or Virus Detection)
  - CSSA/ISSM will:
    - Perform preliminary investigation
    - Implement approved clean-up or maintenance procedures

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



ISSO Responsibilities

Responsibility

Personnel assigned as ISSOs or Alternate ISSOs are responsible for ensuring that system assurance is maintained.

Briefings

The ISSM/CSSA will provide in-depth briefings and training of the ISSO position prior to the assumption of ISSO duties. After briefings and training are completed the CSSA will:

- File signed ISSO Delegation Record in SSP
- File signed Privileged User Briefing in SSP
- Upload signed Privileged User Briefing to SharePoint
- Create account(s) as required
  - Without privileges
  - With elevated privileges
- Grant SharePoint access
- Add ISSO to distribution list

Tasks

- Daily
  - Perform visual inspection of Protected Distribution System (PDS) (if applicable)
    - Report anomalies to CSSA/ISSM
  - Review area for unmarked media, if found, ensure media is marked, stored, and labeled appropriately

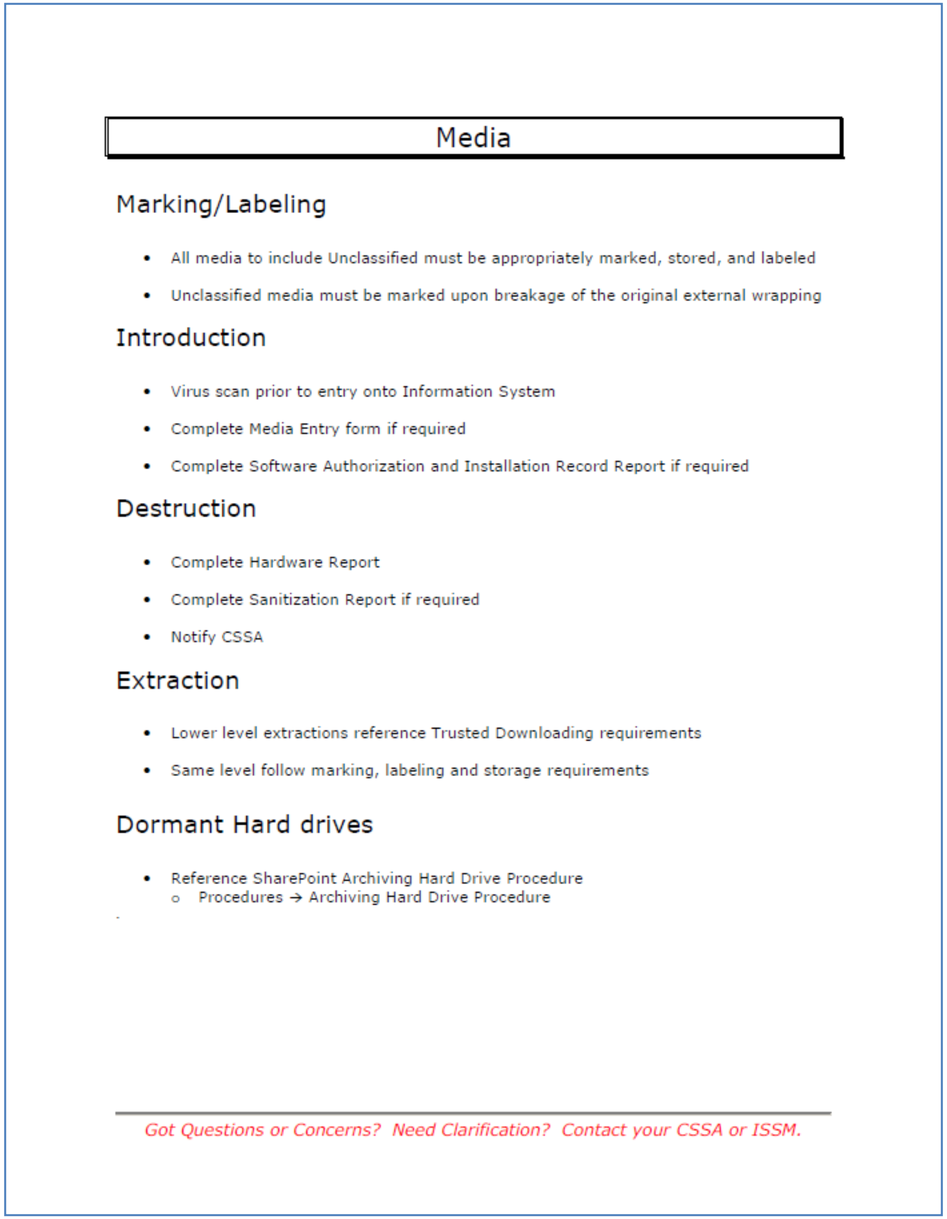
- Weekly
  - Review and/or run audit logs
  - Review SSP Reports and Logs (i.e. Hardware and Software Records, Maintenance and Seal Log, and Sanitization Forms)
  - Review Share Point for new information
  - Complete Weekly Audit Record form

- Monthly
  - Create/Ensure Backup of Audit History
    - Maintain one inspection cycle worth of records
    - Ensure media is marked, stored, and labeled appropriately
      - Remove logs older than 1 inspection cycle
  - Update Windows and Linux Anti-Virus Definition files

- Quarterly
  - Attend ISSO briefings

- Annually
  - Revalidate user accounts and access

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Media

Marking/Labeling

- All media to include Unclassified must be appropriately marked, stored, and labeled
- Unclassified media must be marked upon breakage of the original external wrapping

Introduction

- Virus scan prior to entry onto Information System
- Complete Media Entry form if required
- Complete Software Authorization and Installation Record Report if required

Destruction

- Complete Hardware Report
- Complete Sanitization Report if required
- Notify CSSA

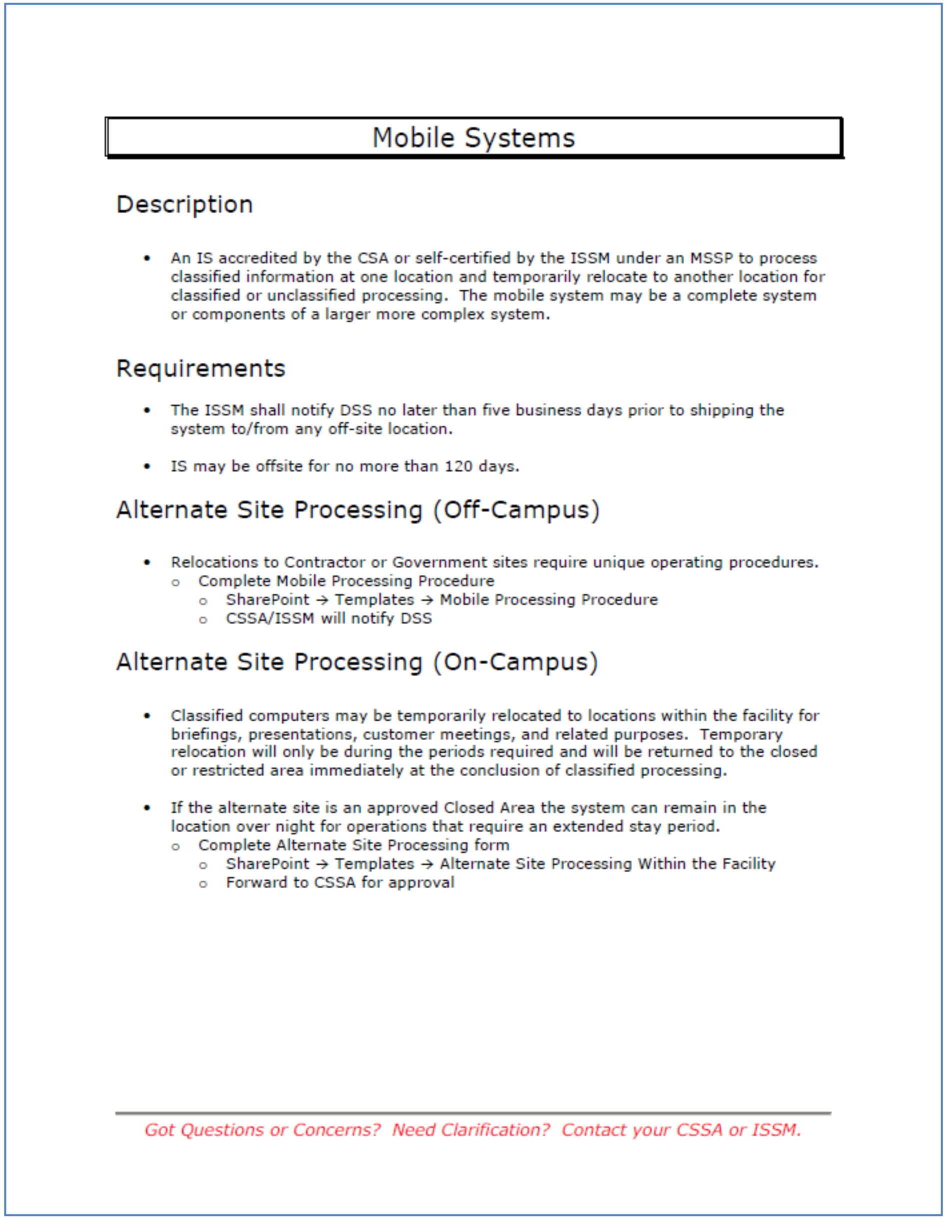
Extraction

- Lower level extractions reference Trusted Downloading requirements
- Same level follow marking, labeling and storage requirements

Dormant Hard drives

- Reference SharePoint Archiving Hard Drive Procedure
  - Procedures → Archiving Hard Drive Procedure

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Mobile Systems

Description

- An IS accredited by the CSA or self-certified by the ISSM under an MSSP to process classified information at one location and temporarily relocate to another location for classified or unclassified processing. The mobile system may be a complete system or components of a larger more complex system.

Requirements

- The ISSM shall notify DSS no later than five business days prior to shipping the system to/from any off-site location.

- IS may be offsite for no more than 120 days.

Alternate Site Processing (Off-Campus)

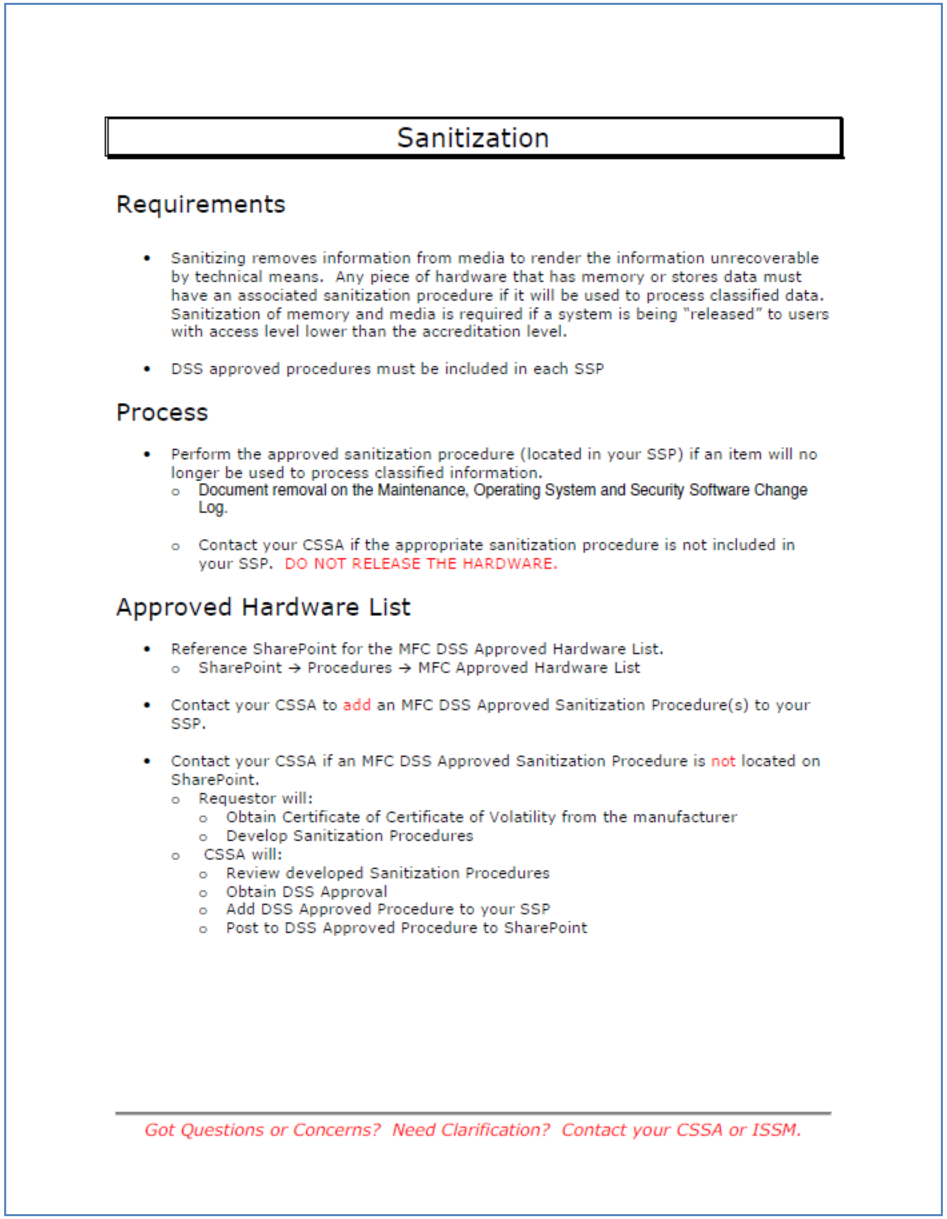
- Relocations to Contractor or Government sites require unique operating procedures.
  - Complete Mobile Processing Procedure
    - SharePoint → Templates → Mobile Processing Procedure
    - CSSA/ISSM will notify DSS

Alternate Site Processing (On-Campus)

- Classified computers may be temporarily relocated to locations within the facility for briefings, presentations, customer meetings, and related purposes. Temporary relocation will only be during the periods required and will be returned to the closed or restricted area immediately at the conclusion of classified processing.

- If the alternate site is an approved Closed Area the system can remain in the location over night for operations that require an extended stay period.
  - Complete Alternate Site Processing form
    - SharePoint → Templates → Alternate Site Processing Within the Facility
    - Forward to CSSA for approval

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Sanitization

Requirements

- Sanitizing removes information from media to render the information unrecoverable by technical means. Any piece of hardware that has memory or stores data must have an associated sanitization procedure if it will be used to process classified data. Sanitization of memory and media is required if a system is being "released" to users with access level lower than the accreditation level.

- DSS approved procedures must be included in each SSP

Process

- Perform the approved sanitization procedure (located in your SSP) if an item will no longer be used to process classified information.
  - Document removal on the Maintenance, Operating System and Security Software Change Log.

  - Contact your CSSA if the appropriate sanitization procedure is not included in your SSP. DO NOT RELEASE THE HARDWARE.

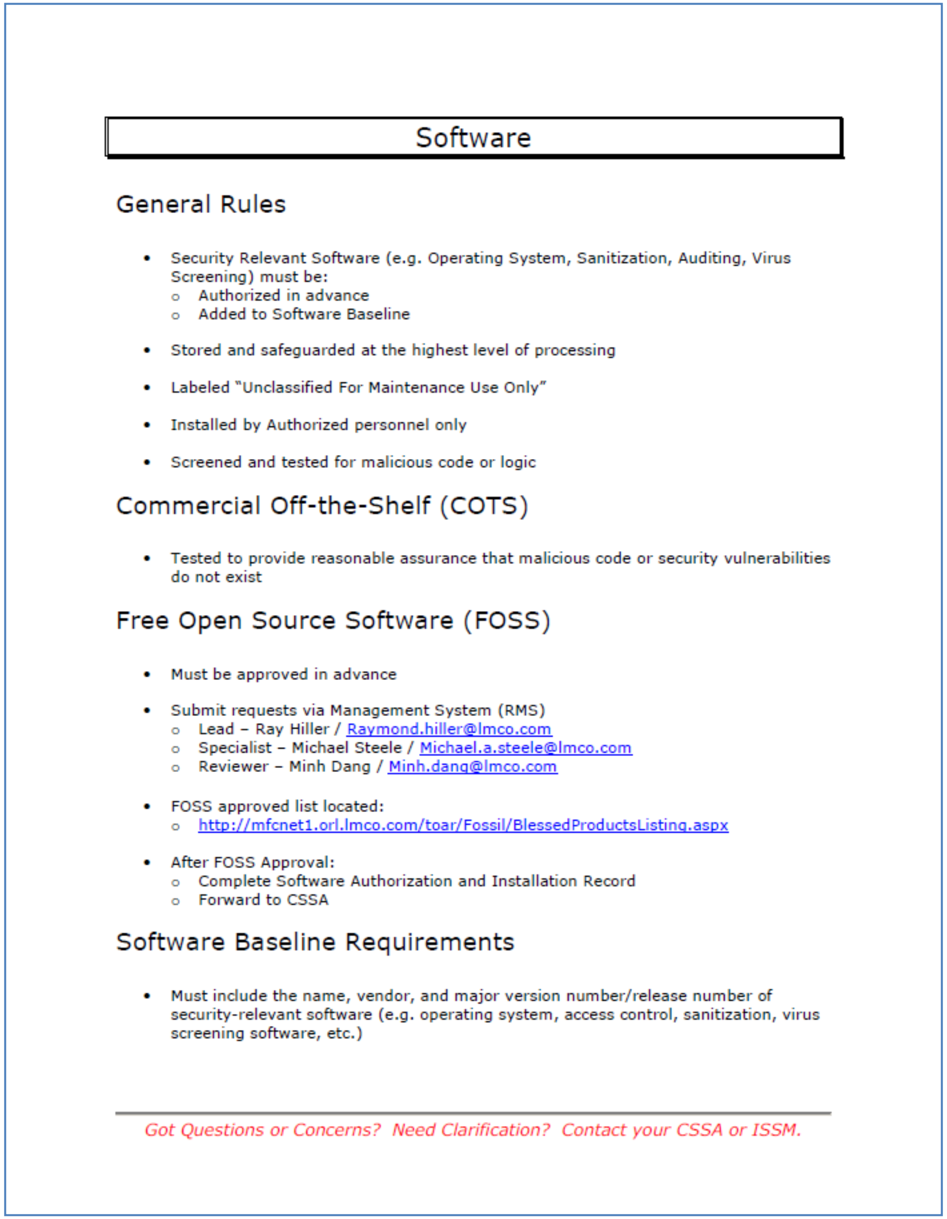
Approved Hardware List

- Reference SharePoint for the MFC DSS Approved Hardware List.
  - SharePoint → Procedures → MFC Approved Hardware List

- Contact your CSSA to add an MFC DSS Approved Sanitization Procedure(s) to your SSP.

- Contact your CSSA if an MFC DSS Approved Sanitization Procedure is not located on SharePoint.
  - Requestor will:
    - Obtain Certificate of Certificate of Volatility from the manufacturer
    - Develop Sanitization Procedures
  - CSSA will:
    - Review developed Sanitization Procedures
    - Obtain DSS Approval
    - Add DSS Approved Procedure to your SSP
    - Post to DSS Approved Procedure to SharePoint

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Software

General Rules

- Security Relevant Software (e.g. Operating System, Sanitization, Auditing, Virus Screening) must be:
  - Authorized in advance
  - Added to Software Baseline
- Stored and safeguarded at the highest level of processing
- Labeled "Unclassified For Maintenance Use Only"
- Installed by Authorized personnel only
- Screened and tested for malicious code or logic

Commercial Off-the-Shelf (COTS)

- Tested to provide reasonable assurance that malicious code or security vulnerabilities do not exist

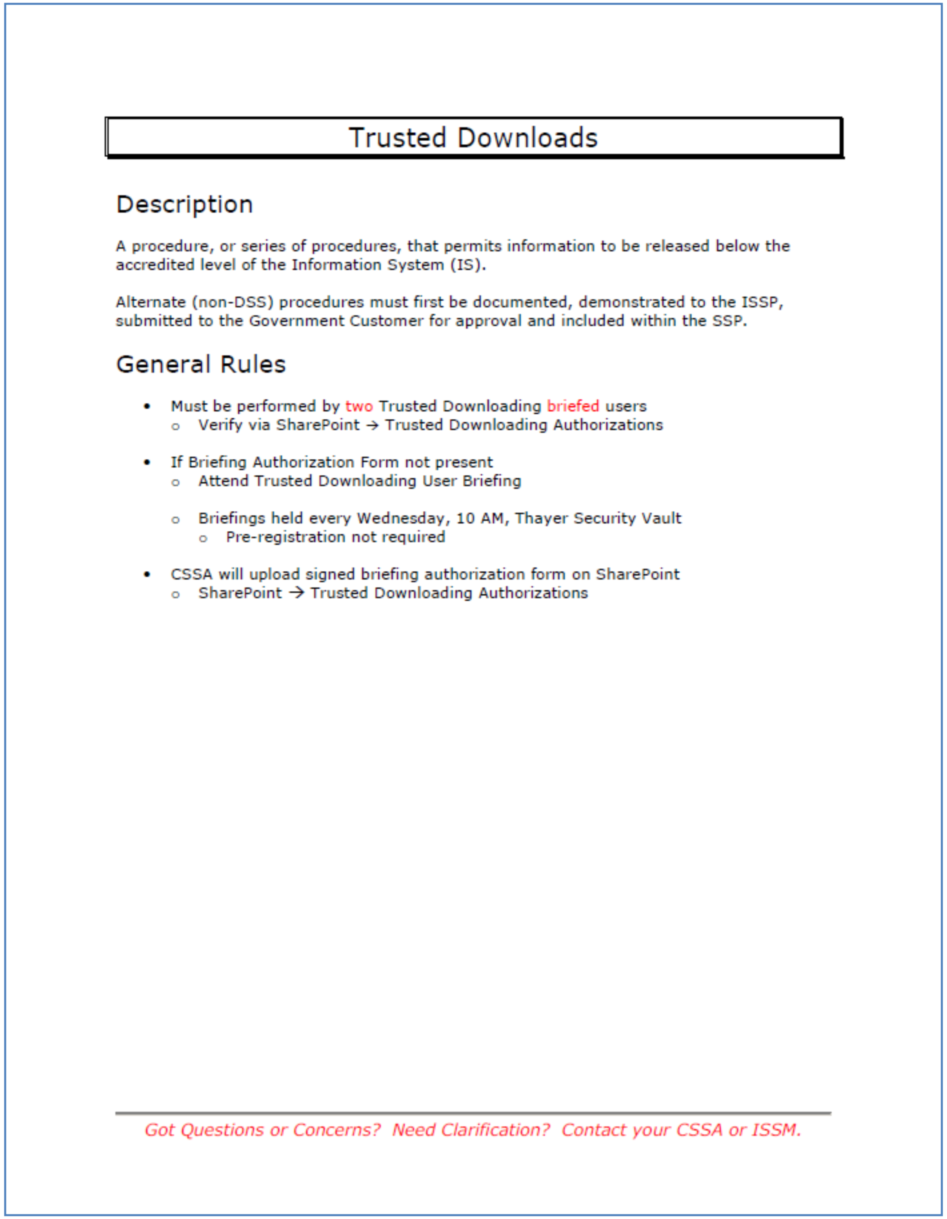
Free Open Source Software (FOSS)

- Must be approved in advance
- Submit requests via Management System (RMS)
  - Lead – Ray Hiller / Raymond.hiller@lmco.com
  - Specialist – Michael Steele / Michael.a.steele@lmco.com
  - Reviewer – Minh Dang / Minh.dang@lmco.com
- FOSS approved list located:
  - http://mfcnet1.orl.lmco.com/toar/Fossil/BlessedProductsListing.aspx
- After FOSS Approval:
  - Complete Software Authorization and Installation Record
  - Forward to CSSA

Software Baseline Requirements

- Must include the name, vendor, and major version number/release number of security-relevant software (e.g. operating system, access control, sanitization, virus screening software, etc.)

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Trusted Downloads

Description

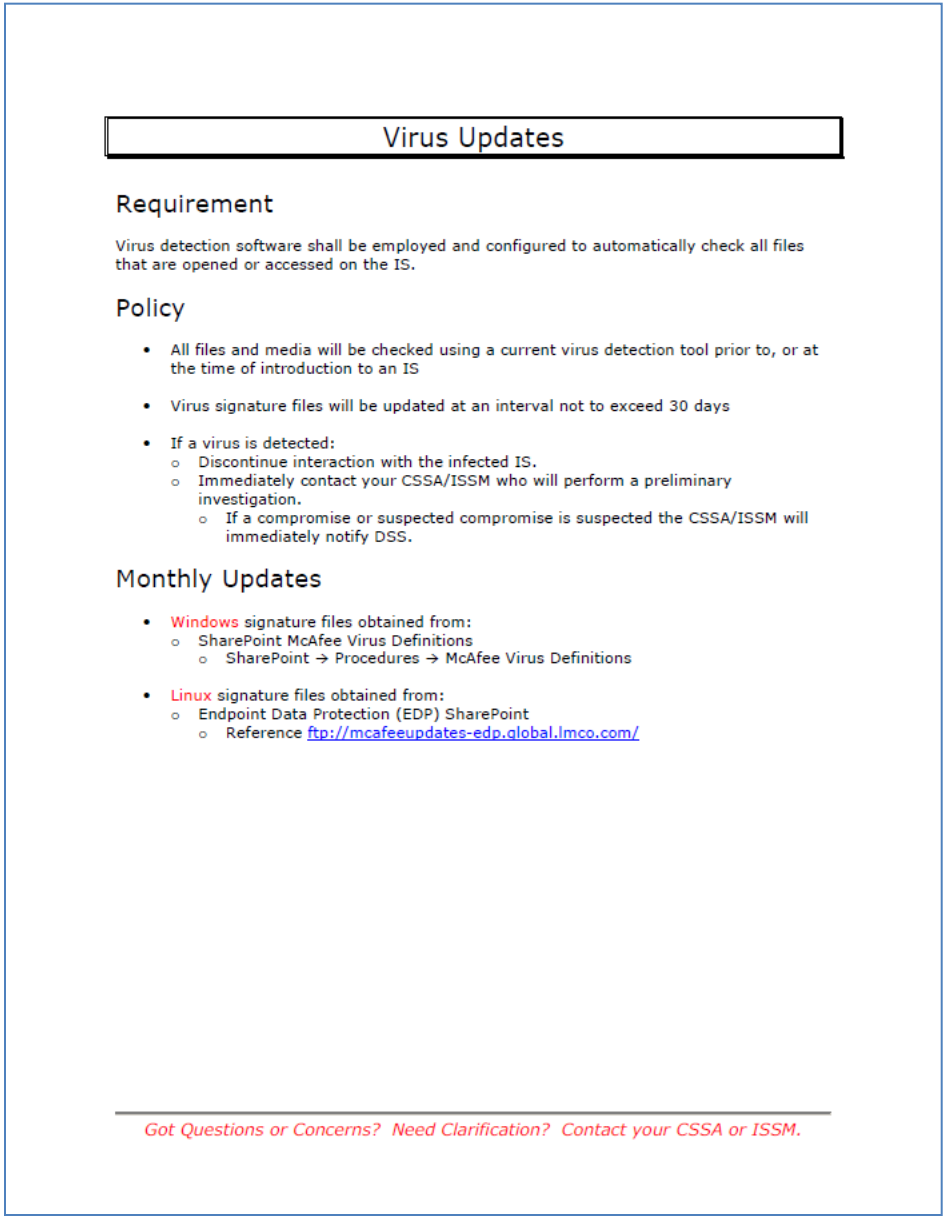
A procedure, or series of procedures, that permits information to be released below the accredited level of the Information System (IS).

Alternate (non-DSS) procedures must first be documented, demonstrated to the ISSP, submitted to the Government Customer for approval and included within the SSP.

General Rules

- Must be performed by two Trusted Downloading briefed users
  - Verify via SharePoint → Trusted Downloading Authorizations
- If Briefing Authorization Form not present
  - Attend Trusted Downloading User Briefing
  - Briefings held every Wednesday, 10 AM, Thayer Security Vault
    - Pre-registration not required
- CSSA will upload signed briefing authorization form on SharePoint
  - SharePoint → Trusted Downloading Authorizations

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.



Virus Updates

Requirement

Virus detection software shall be employed and configured to automatically check all files that are opened or accessed on the IS.

Policy

- All files and media will be checked using a current virus detection tool prior to, or at the time of introduction to an IS
- Virus signature files will be updated at an interval not to exceed 30 days
- If a virus is detected:
  - Discontinue interaction with the infected IS.
  - Immediately contact your CSSA/ISSM who will perform a preliminary investigation.
    - If a compromise or suspected compromise is suspected the CSSA/ISSM will immediately notify DSS.

Monthly Updates

- Windows signature files obtained from:
  - SharePoint McAfee Virus Definitions
    - SharePoint → Procedures → McAfee Virus Definitions
- Linux signature files obtained from:
  - Endpoint Data Protection (EDP) SharePoint
    - Reference ftp://mcafeeupdates-edp.global.lmco.com/

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.

SharePoint

Access

- Site access given to Privileged Users to include but not limited to ISSOs/AISSOs, CSSAs, and System Administrators

Contents

- User Briefing Schedule and Forms, Trusted Downloading Authorizations, Privileged User Authorizations, Termination List
- Forms/Templates – Hardware/Software Records, Seal Logs, Termination Form etc.
- McAfee Virus Definition – Monthly Updates
- Procedures – Sanitization, Hard Drive Marking, Closed Area Marking, Data Spills, etc.
- ISSO Tasks – Daily, Weekly, Monthly, Quarterly and Annual
- Education/Presentations – Auditing Video, ISSO Quarterly Meetings, How to Add a User, etc.

Link

- http://enterprisesecurity.orl.lmco.com/ISSM/ISSO/Shared%20Documents/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fenterprisesecurity%2eorl%2elmco%2ecom%2fISSM%2fISSO%2fShared%20Documents%2fDAL%2dISSO&FolderCTID=0x0120004B7F9A80B3C26A488D8480843D418568

Got Questions or Concerns? Need Clarification? Contact your CSSA or ISSM.

Where do I find that document??
Let me show you