



District of Columbia Pretrial Services Agency

Policy Statement 5560

Policy Area: Information Technology

Effective Date: April 21, 2005

Management Instruction

Approved: 
Ronald L. Hickey
Director, OIT

MEDIA PROTECTION FOR PSA BUSINESS AND MISSION CRITICAL SYSTEMS

I. MANAGEMENT INSTRUCTION

Information that is stored, transferred, distributed, printed, or otherwise duplicated from all District of Columbia Pretrial Services Agency's (PSA) business and mission critical systems, must adhere to media protection control requirements. Controls are required to be implemented and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5510, *Media Protection Policy for PSA Business and Mission Critical Systems*.

II. COVERAGE

This Management Instruction applies to all permanent and temporary PSA employees, including contractors and interns that use, manage, develop, maintain, or support PSA business and mission critical systems. The term employee as used in this management instruction, collectively refers to all of the aforementioned personnel types.

III. BACKGROUND

Media protection control is a set of production and input/output controls for the creation, handling, processing, storage, labeling and distribution of information that resides on fixed or removable electronic or hard copy media. These control measures are designed to protect sensitive information that is stored, handled, transported, or destroyed outside the inherent physically and logically protected boundaries of the information system.

IV. PROCEDURES

A. Definition

This Management Instruction outlines procedures for adequate media protection control. Media protection control employs process supported by formal institutionalized instructions and adequate technology, to protect system information integrity and confidentiality when the information is copied, distributed, or handled - on electronic or hard copy media - outside of a system's physical and logical production boundaries,

Media protection control supports the inherent requirement of contingency planning to maintain current electronic copies of system data and documentation by ensuring the protection of confidentiality, integrity, and availability of the information and system data in the event there is need for restoration and reconstitution.

Media protection control may apply to testing, development, staging, and/or training environments where potential compromise can be correlated to the impact criteria for confidentiality, integrity, and availability in a respective production environment. Table 1, a sample media protection requirements worksheet can be used as guidance for mapping those information types to the level of protection required and for identifying any compensating or mitigating controls that would serve in lieu of normal production environment security requirements.

Table 1. Sample Media Protection Requirements Worksheet

System	Media	Information Type	Impact Consideration	Security Category	Physical Protection	Logical Protection	Verified & Validated
PRISM	PSA Training Environment	Live Data	Confidentiality	Moderate	Separate server but same data center as production.	Personally identifiable information removed and replaced	Yes or no
WinTOX	PSA Staging Environment	Live Data, Pre-deployed app code and db schema	Confidentiality Integrity, Availability	Moderate	Same as Production (same server, data center)	Same as production (same DBMS)	Yes or no

B. Terms

- **Availability** – Assurances that systems and networks (communications) provide adequate capacity to perform in a predictable manner with an acceptable level of performance. Ensures reliability and timely access to information, information systems and information system resources.
- **Business Critical System** - IT system comprised of technology and users within physical and logical boundaries that support the business function of PSA (e.g., a financial management system).

- **Confidentiality** - Assurance that the necessary level of secrecy is enforced at each juncture of information processing and handling. The prevention of unauthorized disclosure.
- **Degaussing** - Erasure of information from a magnetic disk or other storage device.
- **Digital Media, Electronic Form** – Any form of information stored in a computer.
- **Flash Memory** - A rewritable memory chip that holds its content without power. Flash is widely used for storage modules, including USB keychain drives, voice recorders, and digital camera memory cards.
- **Integrity** - Assurances of accuracy and reliability of information and information systems processing. The prevention of unauthorized (intentional or unintentional) modification, deletion, or addition of data/information.
- **Magnetic Media** – Media such as disk or tape that is magnetically recorded and can be re-recorded over and over.
- **Media Sanitization** - To remove data from an information system, a database or an extract from a database.
- **Mission Critical System** – IT system comprised of technology and users within physical and logical boundaries that support organizational missions.
- **Optical Media** – Typically optical media comes in the form of disks. Some disks are read only or write-once and cannot be erased. Others are rewritable. Optical disks have advantages over magnetic disks in that they have higher capacities, are not subject to head crashes or corruption from stray magnetic fields, have a long life and are less vulnerable to extremes of hot and cold.
- **Paper, Hard Copy Media, Printed Form** – Paper or other physical, tangible form that contains written, graphical or pictorial information.
- **Security Categorization (FIPS 199)** - Federal Information Processing Standard that establishes the criteria for categorizing an information system as low, moderate or high, depending on the security requirements of the system and its data. The security categorization is based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
- **Sensitive Information** – Information that requires controls on disclosure. Sensitive information, as determined by an organization, must be protected via policies and procedures.

C. Authority

The Federal Information Security Management Act (FISMA) requires PSA to institute procedures to facilitate the implementation of a Media Protection Policy. The procedures are derived from guidance provided by the National Institute of Standards and Technology Special Publication 800-53, Draft 2, *Recommended Security Controls for Federal Information Systems*.

D. Requirements

The following media protection control procedures are required to be implemented, practiced, and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5510, *Media Protection Policy for PSA Business and Mission Critical Systems*.

The following technical and process requirements meet the minimum baseline for systems with a security categorization of *Moderate*. Deviations from, or enhancements to these baseline procedures, will be documented, with rationale (e.g., compensating controls mitigating factors, risk acceptance, resource constraints, etc.) and approval, in the System's Security Plan (SSP).

Technical Requirements

- Automated physical access control (e.g., a proxy card system) will be used to:
 - Ensure that only authorized personnel can access media storage areas.
 - Log access attempts and access obtained.

Process Requirements

- Access to information in printed form or on digital media removed, transmitted or distributed from the information system will be restricted to authorized users and protected in accordance with PSA Policy Statement # 5501 and Management Instruction #5551, *Access Control for PSA Business and Mission Critical Systems*.
- External labels will be affixed to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information:
 - All digital media, including backup tapes, will be labeled with the distribution limitations, handling guidelines, and applicable security markings; and
 - Cover sheets will be affixed to hard copy media to prevent unauthorized users from viewing information.

- Information system media, both paper and electronic, will be physically and logically controlled and secured based on the security category (based on FIPS 199 determination) of the information. **This includes information stored on testing, development, staging, and training servers.**
 - Access to testing, development, staging and training servers will be limited to personnel who require such access for work-related purposes only.
 - Information system media will be protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
 - Unmarked media will be protected at the highest FIPS 199 security category for the information system until the media are reviewed for mitigating or compensating circumstances or controls, and then appropriately labeled.
 - Physical security containers and storage facilities will be compliant with General Services Administration policy, requirements, and guidance.
- The pickup, receipt, transfer, and delivery of information system media (paper and electronic) will be controlled and restricted to authorized personnel.
- Information system magnetic media will be sanitized using approved equipment, techniques, and procedures.
- Media sanitization actions and equipment/procedures will be tracked, documented, verified and periodically tested to ensure correct performance
- Sanitization will include:
 - Removing all labels, markings, and activity logs; and
 - Degaussing and overwriting memory locations
 - A National Security Agency approved product will be used to degauss media.
- Digital media will be sanitized or destroyed prior to its disposal or release for reuse outside the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.
- Information system hardware and machine readable media will be:
 - Sanitized using approved methods before being released for reuse outside of the organization, or
 - Destroyed:

- Information storage media will be destroyed when no longer needed in accordance with organization-approved methods and organizational policy and procedures.
- Media destruction and disposal actions will be tracked, documented and verified.
- Nonmagnetic media (e.g., compact disks, Flash Memory) will be physically destroyed in a safe and effective manner.
- Inventory and disposition records will be maintained for digital media to ensure control and accountability of organizational information.
- Digital media logs will be used for receipt of system information and will include:
 - The name of the media recipient,
 - The signature of the media recipient,
 - The date/time media is received,
 - The media control number and contents description,
 - Movement or routing information, and
 - If disposed of, the date, time, and method of destruction.

E. Roles and Responsibilities

A current list of roles and responsibilities will be maintained delineating responsibilities for executing, managing, monitoring and enforcing the procedures in this management instruction.

Table 2 – Roles and Responsibilities

Role	Media Protection (MP) Responsibilities
System Manager	<ul style="list-style-type: none"> • Determines media protection requirements in association with Business Owner. • Ensures MP Management Instruction technical and process controls are implemented.
Business Owner	<ul style="list-style-type: none"> • Determines media protection requirements in association with System Manager.
System Security Officer	<ul style="list-style-type: none"> • Ensures MP Management Instruction requirements are adhered to and monitored.
Media Protection Manager	<ul style="list-style-type: none"> • Coordinates with System Manager for any technical implementations. • Responsible for media sanitization and destruction activities.
System Programmers	<ul style="list-style-type: none"> • Coordinate with System Manager for any technical implementations. • Implement and validate technical controls.
IT support personnel	<ul style="list-style-type: none"> • Handles removable backup and other media in accordance with this management instruction.
System users	<ul style="list-style-type: none"> • Read and agree to Rules of Behavior regarding Media Protection.

F. Authorities and References

- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A130, Appendix III
- Federal Information Processing Standards Publication (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems
- The US Privacy Act of 1974
- CSOSA Memorandum: *Standards of Employee Conduct*, Effective August 30, 1999
- CSOSA and PSA Policy Statement 4007: *Release of Defendant/Offender Drug Test Information*, Effective July 28, 2004
- PSA Policy Statement #5500, *PSA Global Information Technology Security Policy*
- PSA Policy Statement #5510, *Media Protection Policy for PSA Business and Mission Critical Systems*
- PSA Policy Statement #5506, *Contingency Planning Policy for PSA Business and Mission Critical Systems*
- PSA Management Instruction, Policy Statement #5556, *Contingency Planning for PSA Business and Mission Critical Systems*
- Guide for the Security Certification and Accreditation of Federal Information Systems (NIST SP 800-37)
- Recommended Security Controls for Federal Information Systems (NIST SP 800-53)
- Risk Management Guide For Information Technology Systems (NIST SP 800-30)
- An Introduction To Computer Security – The NIST Handbook (NIST SP 800-12)

G. Attachments

- DC. Pretrial Services Agency Office of Information Technology System and Tape Backup Procedure, January 25, 2005
- Security Control Reference Guide