MEDIA MANAGEMENT

ISSP-31-0410

1. **SUBJECT:** Media must be handled, stored, and disposed of properly in order to protect the sensitive or critical OPIC data stored upon it.
2. **SCOPE:** This policy applies to all media that is used to store OPIC data.
3. **DESCRIPTION:** OPIC has been entrusted with a variety of sensitive data in order to accomplish its mission. This data, which is stored on a variety of media, must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, OPIC will use a variety of security mechanisms that provide protections for media.
4. **PROCEDURES & GUIDELINES:**

   (a) Media Handling:

   (1) Users should take all reasonable steps to protect OPIC storage media in their possession from tampering or accidental damage.

   (2) Users are responsible for making their own backups of any data that is not stored on OPIC servers.

   (3) Appropriate physical and environmental protection controls shall be provided for stored media.

   (4) Handling media that contain sensitive data:

   - Any media containing sensitive data should be marked with its classification level. Labeling shall include any special handling instructions
   - Any media containing sensitive data must be secured (such as kept in a locked drawer, cabinet, or safe) when not in use or unattended. Any media sensitive information transported through the mail or courier/messenger service shall be double-sealed, the second envelope shall be appropriately marked with the sensitivity classification of the data.
   - The receipt and delivery of media containing sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.
   - Sensitive information shall be turned over or shall be put out of sight when visitors are present.

   (b) Media Disposal:

   (1) Information Users need to understand that simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly.

(2) Media that contain sensitive data must be sanitized when they are no longer needed to store the sensitive data.

(3) Before any OPIC-owned or managed computing equipment is transferred, donated, or otherwise disposed of, storage media associated with the equipment must be sanitized via approved government methods.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any media they own, and media that contains data or applications that they own, are handled and disposed of in accordance with OPIC policies and procedures.

(b) Information Custodians are responsible for:

(1) Assisting information owners with the proper handling of their media in accordance with OPIC policies and procedures.

(2) Complying with OPIC policies and procedures for any media entrusted to them.

(3) Reporting the loss, damage, or theft of any media entrusted to them that contains OPIC data.

(c) Information Users are responsible for:

(1) Protecting OPIC media in their possession from tampering or accidental damage.

(2) Storing OPIC data only on approved media.

(3) Backing up data that is stored on media in their physical possession.

(4) Reporting the loss, damage, or theft of any media containing OPIC data.

(d) Supervisors are responsible for:

(1) Ensuring that their employees understand how to properly handle and dispose of media in accordance with OPIC policies and procedures.

(2) Communicating changes in policies and procedures to their staff.

(e) The Information Systems Security Officer (ISSO) is responsible for developing media management standards and performing auditing to ensure that media is being handled and disposed of in accordance with OPIC policies and procedures.

6. DEFINITIONS:

(a) Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.

(b) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(c) Sanitization - To expunge data from storage media so that data recovery is impossible. The most common types of sanitization are destruction (*e.g.* burning or smashing), degaussing (*i.e.* demagnetizing), and overwriting.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.
8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)
9. **ATTACHMENTS:** None
10. **AUTHORITY:**

    (a) OPIC Directive 00-01, Information Systems Security Program.

    (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

    (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

    (d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

    (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

    (f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

    (g) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

    (h) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

11. **LOCATION:** TBD
12. **EFFECTIVE DATE:** October 22, 2004
13. **REVISION HISTORY:** None
14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.