

DATE March 25, 2004

INFORMATION TECHNOLOGY STORAGE MEDIA CONTROLS

1. PURPOSE AND SCOPE. This circular establishes policy and defines responsibilities for the protection of all digital media and paper-based input to, or output from Information Technology (IT) systems that contain sensitive but unclassified information. This policy applies to all Bureau employees, contractors, and others who use information technology to process, store or transmit Bureau information.

2. POLICY. It is the policy of the Bureau to protect the confidentiality, integrity, and availability of sensitive information in compliance with the Treasury Information Security Program Policy, TD P 85-01, and other Department of the Treasury and Federal policies and regulations.

a. Media Protection. All media and paper-based system input and output containing sensitive information shall be stored in a secure location when not in use. Controls to protect information systems, input and output shall be implemented for storing, handling, and destroying media and paper documents to ensure that sensitive information cannot be accessed by unauthorized individuals. This policy establishes minimum controls. However, additional controls may be mandated and documented in applicable Information Technology System Security Plans (System Security Plans). Backup media shall be stored at an offsite location having appropriate security controls in accordance with contingency plans.

Logs will be used to maintain accountability and to track media deposited in and withdrawn from media storage facilities and libraries. An accurate chain of custody will be maintained and users will be held accountable for media removed from storage.

Unless the Office of Critical Infrastructure and Information Technology Security has provided a written determination that specific information is not sensitive, all Bureau data must, at a minimum, be provided the same level of protection afforded sensitive data.

b. Media Marking. Limited Official Use information must be marked in compliance with BEP Manual No. 71-00.42, "Information Security Manual." All removable media containing Limited Official Use information must have warning labels affixed, the same as those required for diskettes.

c. Sanitization. Prior to disposal, any device containing a hard drive or memory that has processed sensitive information shall be sanitized, portable electronic devices shall be destroyed, and sensitive media shall be sanitized or destroyed according to established procedures.

DATE March 25, 2004

Sensitive information stored on media which is to be surplus or returned to the manufacturer shall be purged before leaving the Bureau. Disposal shall be performed using approved sanitization methods which are commensurate with the sensitivity of the data residing on these devices. Records shall be maintained certifying that such sanitization was performed.

d. Disposal. Disposition of official records must be handled according to the appropriate Bureau or other Records Schedule. Electronic information, files, and documents are records just as paper documents are.

Upon the termination or reassignment of an employee, sensitive information stored on any media used by this employee, shall be transferred to his/her supervisor. If a contractor is terminated or reassigned, information shall similarly be transferred to the supervisor and, upon contract termination, transferred to the COTR.

Sensitive information shall be purged from the hard drives of any computer workstation or server which is returned to the surplus pool of equipment, re-deployed, or transferred to another individual. This shall be done in such a manner that the information on that media cannot be recovered by ordinary means. Examples of acceptable methods of disposal are crosscut or strip shredders, degaussing, and approved disk-wiping software.

3. REFERENCES.

a. "Treasury Information Technology Security Program," Treasury Directive Publication (TD P) 85-01, Volume I Policy, Part 1 "Sensitive Systems," dated August 15, 2003.

b. "Department of Treasury Security Manual," Treasury Directive Publication (TD P) 71-10.

c. BEP Manual No. 71-00.42, "Information Security Manual," dated March 16, 2000.

d. Privacy Act of 1974, 5 United States Code (USC) Section 552a.

e. Federal Information Processing Standard Publication 199 (FIPS Pub 199) "Standards for Security Categorization of Federal Information and Information Systems."

4. DEFINITIONS.

a. Availability. Timely, reliable access to data and information services for authorized users. This includes the restoration of services after an interruption.

DATE March 25, 2004

b. Bureau System. An IT system (including telecommunications, networks, computers, and software programs) that is owned, leased, or operated by the Bureau or is operated by a contractor or another government agency on behalf of the Bureau.

c. Confidentiality. The assurance that information is not disclosed to unauthorized persons, processes, or devices.

d. Highly sensitive information. FIPS Pub 199 defines three levels of potential impact on organizations or individuals should there be a loss of confidentiality, integrity or availability. Information for which the potential impact is moderate or high is considered to be highly sensitive information. Most information is in the low potential impact category. Minimum security measures are designed to protect information at that level. Additional controls may be required for information that requires a higher level of assurance for confidentiality, integrity, or availability.

e. Integrity. The quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of data structures and occurrence of stored data. Generally, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

f. Storage Media (Media). Objects used to magnetically, optically, or by other means store data. This includes internal, external, and removable storage devices (e.g., hard drives, tapes, diskettes, compact disks, and removable disk drives); master copies of software; and backup files, data, and programs.

g. Media Storage Facilities and Libraries. Environmentally and physically protected on-site or offsite facilities used to store system backup media and master copies of software.

h. Records Schedule. A document that describes agency records, establishes a period for their retention by the agency, and provides mandatory instructions for what to do with them when they are no longer needed for current government business.

i. Sanitization. Elimination of sensitive information from an information technology system or media associated with an IT system.

j. Sensitive information. Any information, the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy. The terms "loss," "misuse," and

DATE March 25, 2004

“unauthorized access” can involve unauthorized manipulation of data, destruction or loss of data, denial of service, inability to complete or perform a mission, or willful or negligent disclosure of information.

k. Secure location. A physical and/or logical location that provides adequate controls to protect the confidentiality, integrity and availability of the information. The level of protection required is based upon the sensitivity of the information. Adequate controls result in an acceptable level of risk.

l. System Owner. The information system owner is the program manager responsible for ensuring that the IT system meets the program area functional requirements and approving changes to application requirements. Responsibilities include developing the security plan, ensuring the system is deployed and operated according to the security requirements documented in the plan, and accepting the residual risk to the program of operating the IT system.

m. Unauthorized Disclosure. Exposure of information to persons, processes, or devices not authorized to receive it.

5. RESPONSIBILITIES.

a. Associate Directors, Designated Accrediting Authorities, Plant Managers and Office Chiefs shall:

(1) Determine the level of sensitivity of information; ensure that systems meet Federal, Treasury, and Bureau IT security requirements; and ensure that necessary safeguards are in place to adequately protect the availability, integrity and confidentiality of Bureau information and systems that support their program areas.

(2) Require that all contracts with external companies for repair or recovery of data from systems, hard drives, or media include a nondisclosure statement in accordance with TD P 71-10, Chapter II, Section 2, “Investigative Requirements for Contract Employees.”

b. System Owners shall:

(1) Treat all BEP information as “sensitive” unless specifically designated as “nonsensitive” by the Office of Critical Infrastructure and IT Security.

(2) Notify the Office of Critical Infrastructure and IT Security of any “highly sensitive” information processed on Bureau systems or stored on removable media. Ensure that the relevant System Security Plans document security requirements and procedures for this type of information. These requirements and procedures exceed the minimum requirements and procedures stated in this policy.

DATE March 25, 2004

(3) Ensure that media used to store sensitive information and printed system output are protected in compliance with Bureau policy and procedures.

(4) Ensure that system backup media and master copies of software are stored in a secure media storage facility.

c. Supervisors and COTRs shall:

(1) Ensure that their employees and contractors are aware of and comply with policy and procedures for protecting sensitive information on printed system output and electronic media.

(2) Ensure that sensitive information which has been created and/or maintained by an employee or contractor is transferred to an authorized individual upon the termination or reassignment of the employee or contractor. Submit a Special Access Request (BEP Form 8393) to the IT Security Division to request the transfer of information which is protected by access controls.

d. Users shall:

(1) Protect media and paper system input and output that contain sensitive information to prevent unauthorized disclosure, modification, loss or destruction. Ensure that this information is stored in a secure location, such as a locked desk, bookcase, or room, when not in use.

(2) Ensure that only authorized users access, transport, or store media and paper documents that are used as a source of input to, or are output from, information systems. Minimum standards for protection include:

(a) never leaving a printer unattended when it is located in an area that would allow unauthorized disclosure of the material being printed. Printed material (whether sensitive or not) should be picked up from a local or network printer right away;

(b) using locked bins, sealed envelopes, or 'in person' delivery for distribution of paper input and output; 'in person' delivery or use of sealed envelopes to transport media; and use of sealed envelopes when mailing media, or printed input or output.

(3) Observe special precautions when sensitive information is to be faxed, by first calling the fax destination to ensure that an authorized person will be available to pick up the fax right away.

DATE March 25, 2004

(4) Comply with Bureau policy and procedures for marking media containing officially limited information.

(5) Ensure that media is sanitized in compliance with approved procedures before the transfer, reuse, surplus, or donation of any equipment or media. Compliance with sanitization methods specified in the related System Security Plan is mandatory. If sanitization methods are not specified in the related System Security Plan, the following procedures are approved for sanitization prior to disposal in a regular trash container:

(a) diskettes must be shredded or cut into strips and compact disks must be rendered unreadable by deep scratching on the data side (the shiny side without the label) with a nail, screwdriver or similar tool. Two deep radial scratches extending from the small inner hole to the outer edge are sufficient.

(b) All other media must be transferred to the Office of Information Technology Operations for sanitization.

(6) Ensure that sensitive information removed from an information system in printed form is disposed of in compliance with approved disposal methods. Compliance with destruction methods specified in the related System Security Plan is mandatory. Printed output must be disposed of in a manner that does not allow unauthorized disclosure. If destruction methods are not specified in the related System Security Plan, the following methods are approved for disposal:

(a) public information and information for which access is not restricted in any way may be recycled or discarded in a regular trash container;

(b) all other printed information must be shredded using a crosscut or strip shredder.

e. System Administrators shall:

(1) Ensure that system backup media and master copies of software are stored in a secure media storage facility.

(2) Maintain records to track the deposits and withdrawals from media storage facilities and libraries, and the receipt of media that are transferred to another location by courier or mail. Maintain the official chain of custody for the media and hold user's accountable for media removed from storage. Secure records to prevent unauthorized access and manipulation of log information.

(3) Comply with procedures for sanitizing all electronic media, hard disks, memory, or other storage devices containing sensitive data or software before the

DATE March 25, 2004

transfer, reuse, dispatch to external organization for maintenance or replacement, surplus, donation or disposal of any equipment or media.

(4) Comply with procedures to certify that sanitization was performed, and maintain and provide records certifying that sanitization was done.

f. Office of Administrative Services shall:

(1) Comply with procedures for ensuring that any device containing a hard drive or memory has been sanitized before being donated or placed on surplus.

g. The Office of Information Technology Operations shall:

(1) Ensure that system backup media, and master copies of software are stored in a secure media storage facility.

(2) Comply with procedures for sanitizing all electronic media, hard disks, memory, or other storage devices containing sensitive data or software before the transfer, reuse, dispatch to external organization for maintenance or replacement, surplus, donation or disposal of any equipment or media.

(3) Comply with procedures to certify that sanitization was performed, and maintain and provide records certifying that sanitization was done.

h. The Office of Critical Infrastructure and Information Technology Security shall:

(1) Establish policy, procedures, and standards for media controls, media protection, media marking, production input/output controls, sanitization, and disposal to ensure protection of the Bureau's information throughout the systems lifecycle.

(2) Provide oversight to ensure compliance with policy, procedures, and standards for media controls.

(3) Evaluate highly sensitive information and recommend appropriate media controls.

(4) Establish procedures to ensure sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.

(5) Maintain records of authorized exceptions and waivers to IT security policies, procedures and standards for media controls.

CIRCULAR

DATE March 25, 2004

- 6. SANCTIONS FOR MISUSE.** Failure to protect the confidentiality, integrity, and availability of sensitive information may result in suspension of privileges, disciplinary action (up to and including removal), and/or criminal prosecution depending on the nature and severity of the misuse.
- 7. EXCEPTIONS AND WAIVERS.** Exceptions and waivers to this policy require that a written request be submitted to the Chief, Office of Critical Infrastructure and Information Technology Security. Bureau Chief Information Officer (CIO) approval must be received before implementing an exception to, or waiver of, this policy.
- 8. OFFICE OF PRIMARY RESPONSIBILITY.** Associate Director (Chief Information Officer).

<SIGNED>

Ronald W. Falter

Associate Director (Chief Information Officer)

DISTRIBUTION – E