pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Data Cleansing

ITP Number	***Effective Date***
ITP-SEC015	May 1, 2013
Category	***Supersedes***
Recommended Policy	ITP-SYM009
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	May, 2014

This ITP establishes policy, responsibilities, and procedures for the sanitization and/or destruction of leased or state-owned computer system drives, removable media and hand-held devices.

1. Purpose

To establish policy, responsibilities, and procedures for the sanitization and/or destruction of leased or state-owned computer system drives, removable media and hand-held devices.

2. Scope

This ITP applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

Degaussing: a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field.

Disk Wipe: a procedure that uses a single character to overwrite all addressable locations on a hard drive.

DoD 5220.22-M: DoD clearing standards, as identified in DoD 5220.22-M, requires three passes where the entire hard drive is overwritten.

DoD: U.S. Department of Defense.

DoD Rated Degausser: DoD Type degaussers that meet or exceed DoD Type I or Type II media sanitization standards.

DoD Type I Degausser: equipment rated to degauss magnetic media having a maximum coercivity of 350 oersteds.

DoD Type II Degausser - Type II Degaussers: equipment rated to degauss magnetic media having a maximum coercivity of 750 oersteds.

Hard Drive: or "hard disk" is a rigid metal disk coated with a magnetic material on which data for a computer can be stored.

NSA Rated Degausser: a degausser that conforms to NSA/CSS Specification L1-MTC-4A standards for secure erasure.

4. Objective

Provide required actions for agencies to follow for data cleansing.

5. Policy

This policy was developed in collaboration with Agency Chief Information Officers and IT Managers, the Office of Administration and the Department of General Services. This policy applies to all agencies under the governor's jurisdiction. It will take effect immediately, and applies to equipment that is:

- Owned or leased by agencies
- Used by contractors on behalf of the Commonwealth

Citizen and agency data are to be securely erased and storage media physically removed from state-owned and leased devices in accordance with policies outlined in this IT Policy.

Peripheral storage devices including but not limited to floppy diskettes, CD and DVD discs along with external storage devices such as USB drives, are not to be used by end users for storing Commonwealth data. An exception may be made for specific tasks only if the user is directed to do so by his or her agency's IT staff or administrator. In such cases the external storage media used are to follow the same guidelines as hard drives for purging data or be physically removed and destroyed once retired or decommissioned. This also includes archive media such as tape backup. Please refer to the "NIST Guidelines for Media Sanitization" (Draft SP 800-88) document for acceptable destruction procedures.

In addition, wireless handheld devices are to have the capability to perform an erase procedure remotely from a server so that data confidentiality can be maintained even in the event where a user's device is lost or stolen.

I. Proper Disposal of Retired State-Owned Computers

1. Degauss, Wipe, or Destroy the Hard Drives. All data residing on a physical hard drive is to be destroyed in accordance with the "NIST Guidelines for Media Sanitization" (Draft SP 800-88) or be securely erased by using either an NSA or DoD rated degausser, or by performing a DoD 5220.22-M wipe where data is overwritten using a three pass approach. If an agency is leasing Dell computers then it is suggested that the agency take advantage of the prepaid disk wipe service offered by Dell.

2. Recycle Non-Functional Computers. Wiped or degaussed hard drives that no longer contain Commonwealth data and chain of custody are not an issue. Hard drives already removed from the PCs can be destroyed or recycled by the agency, or packaged and sent to the DGS Recycling Office

3. Surplus Functional Computers. The DGS Bureau of Supplies and Surplus Operations can facilitate reutilization or sales of functional computers without hard drives. Consult the agency's Property Control Officer (PCO) to make online surplus system entries; to fill out an identification tag for the users' computers; and to arrange for transportation to DGS. User entries to the online system and physical identification tag are to indicate the type of hard drive, if any, and method used to remove data (i.e., ATA HD-Secure Erase, IDE HD - DoD 5220.22-M triple wipe, no HD, etc.).

4. Package/Palletize the Computer Equipment. Agencies are to package the equipment for shipment. Wiped hard drives should be packaged separately. Please make arrangements for collection or delivery with the DGS Bureau of Supplies and Surplus at (717) 787-6159 Shipments to DGS Bureau of Supplies and Surplus are to also be suitably packaged and labeled

5. Store in a Secure Location. The equipment is to be stored in a secure location pending delivery or collection

II. Proper Return of State-Leased Computers

Note: The Department of General Services (DGS) has issued the following state-wide Contracts 4400012495 (HP), 4400012497 (Pomeroy IT Solutions), 4400012505 (CDW), 4400012506 (Synnex Corp), 4400012507 (Dell) that include information regarding disk wiping services provided by these vendors: If the agency leases equipment, it is suggested that the agency utilize this prepaid service. No value will be returned to the Commonwealth if this service is used for Commonwealth-owned computers.

1. Degauss or Wipe the Hard Drive. All data residing on a physical hard drive is to be securely erased using an NSA or DoD rated degausser or by

performing a DoD 5220.22-M wipe where data is overwritten using a three pass approach. ***If an agency is leasing Dell computers, then it is currently required that the agency take advantage of the prepaid disk wipe service offered by Dell when returning leased Dell computers.***

2. Return the leased Computer. Once the drives have been securely erased, they can be reinserted back into the PC or laptop to be returned with the computer to the vendor/contractor as dictated by the leasing agreement.

Note: Be advised that if using the wiping method to securely erase data, then the status log is to be checked each time the process is completed to ensure that the entire disk wiping procedure finished successfully without any errors. Disk wiping is a time-consuming and labor-intensive process that demands high levels of quality control review by IT staff. The agency is fully responsible and liable for taking the necessary measures to ensure that data is securely erased.

III. Computers Owned by Contractors and Used on Behalf of the Commonwealth

Contractor owned computers that are used to perform work for the Commonwealth are to be treated as confidential. Once a contractor has completed his/her engagement, all computer equipment utilized for the engagement is to be securely erased in accordance with the steps below. This can be done by the contractor, a Commonwealth employee or a third party, however, successful completion of this process is to be verified by a Commonwealth employee.

1. Wipe the Hard Drive. All data residing on a physical hard drive is to be wiped by performing a DOD 5220.22-M where data is overwritten using the three pass approach. ***Do not use a degausser for this scenario***. Hard drives that are degaussed are not readily usable as they would require a low-level factory format in order to be reused.

2. Re-image Hard Drive. It is the responsibility of the contractor to re-image or manually reinstall the OS and software applications. The contractor is to be made aware of this policy before he begins an engagement with the Commonwealth.

IV. Reassignment of State-Owned PCs Between Employees of the Commonwealth

1. Wipe the Hard Drive. All data residing on a physical hard drive is to be wiped by performing a DOD 5220.22-M wipe where data is overwritten using a three pass approach. If an agency is leasing computers, please refer to Section II. Proper Return of State-Leased Computers for guidance. ***Do not use a***

degausser for this scenario. Hard drives that are degaussed are not readily usable as they would require a low-level factory format in order to be reused if they have not been damaged.

2. Re-image Hard Drive. Once the hard drive has been wiped, use a backup image such as a Norton Ghost image to reinstall the OS and software applications. It is necessary to wipe prior to re-imaging a computer because imaging does not overwrite the files and data contained in unused areas of a hard drive.

Note: Special cases may exist that do not warrant a DoD disk wipe upon reassignment of a computer between users of Commonwealth owned PCs. In such cases, a Commonwealth department manager has the discretion to determine and request that the wipe procedure not be utilized. By allowing special-case discretion to management, the Commonwealth will be able to promote business efficiency and prevent unnecessary work from being done, while at the same time, not compromising its ability to maintain the confidentiality of its sensitive and private data.

V. Failed Hard Drives and Devices

Whether the equipment or device is state-owned, contractor-owned or leased, all hard drives or media that fail due to a physical malfunction are to be destroyed. If a contractor has a "Statement of Destroyed Materials" or similar policy/program, the agency will not be required to pay for the replacement of the destroyed hard drive. This policy recognizes that a drive contains confidential, sensitive data and cannot be returned. The contractor will credit the Commonwealth as if the drive had been returned.

VI. Multifunction Fax/Print/Scanner Devices

Many multifunction devices now have a presence on the Commonwealth MAN and can contain storage media such as a hard drive. These devices are therefore subject to the same data cleansing policies as outlined above.

VII. DGS Equipment Handling

Equipment delivered to, or collected by, DGS will be taken to a central storage location. At that point, equipment will be held until it is forwarded to the recycler, claimed by and shipped to another agency, or sold. Agencies may deliver non-functional equipment to the recycler by their own means via agency trucks or contracted movers, after they have conformed to the removal and/or secure erase procedures as outlined above and remanded to DGS the Media Disposal Log mentioned above.

6. Responsibilities

Agencies are required to perform the actions outlined in this policy.

7. Related ITPs/Other References

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov. Questions regarding this publication are to be directed to ra-itcentral@pa.gov.

Version	Date	Purpose of Revision
Original		Base Document
Revision	5/1/13	Includes all mobile devices, rescinds ITP-SYM009.
Revision	3/26/14	Updated Section II. Proper Return of State-Leased Computers with updated State Contract numbers and eMarketplace links.