HAMPTON VA

No. IT– 034	Policy Name: Data Disposal Policy
Effective Date: 7-1-2011 Last Revised Date: 7-5-2014	Citywide Policy X IT Policy _ IT Procedure _
Approved By: IT Director	

Data Disposal Policy

Description:

At equipment end of life, the City shall follow procedures to ensure the removal of City data from media resources prior to it being surplused, recycled or transferred to a public computing center or non-city entity, user or function. This procedure prevents unauthorized use of misuse of City information and promotes the privacy and security of sensitive and/or confidential information resources. The procedure also ensures the City is in compliance with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach Bliley Act (aka, Financial Services Modernization Act), IRS 1075 and the Family Educational Rights and Privacy Act.

The City's procedure for removal of City data from electronic media is the process of removing programs or data files on electronic media in a manner that gives assurance that the information cannot be recovered.

The procedure applies to all electronic media that has memory such as hard drives personal computers and laptops, mainframes, Personal Digital Assistants (PDAs), tablet computers, copiers, routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, printers, USBs and other data storage devices.

Background: The risks are related to potential violation of software license agreements, unauthorized disclosure of information such as personally identifiable information, trade secrets, copyrights, and other intellectual property that might be stored on the electronic media. All electronic media containing City data stored on City assets shall have all of that City data securely removed from the electronic media as specified by this standard before the electronic media is surplused, traded-in, otherwise disposed of, or replaced.

Removal of data in the past might have been accomplished by using the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures gave users a sense of confidence

that their data had been completely removed. When using the FORMAT command, Windows displays a message such as:

Important: Formatting a disk removes all information from the disk.

The FORMAT utility creates a new FAT or root tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced FAT and ROOT tables are stored, so that the UNFORMAT command can be used to restore them. FDISK merely cleans the PARTITION TABLE (located in the drive's first sector) and does not remove anything else. In recent years advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped or cleared. Free and commercial software exists that use techniques such as Partial Response Maximum Likelihood (PRML), Magnetic Force Microscopy (MFM) and other recovery methods based on patterns in erased bands to recover cleared data.

Failure to effectively remove the City data could result in a violation of laws and regulations including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Family Educational Rights and Privacy Act (FERPA), IRS 1075, etc.

Acceptable Methods of Data Removal: There are three acceptable methods to be used for the hard drives:

Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or when City data cannot be removed. Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data.

Overwriting – Overwriting is an approved method for removal. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process shall be correctly understood and carefully implemented.

Degaussing – Degaussing is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

The method used for removal of City data, depends upon the operability of the hard drive:
• Operable hard drives that will be reused shall be overwritten prior to disposition. If the operable hard drive is to be removed from service completely and has no value for surplus, it shall be physically destroyed or degaussed.
• If the hard drive is inoperable or has reached the end of its useful life, it shall be physically destroyed or degaussed.

Clearing data (deleting files) removes information from electronic media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing City data from a department device that will be utilized outside of City department or for public or non-City functions. Clearing data may be used for devices being transferred from one City department to another but still being used by internal and non-public facing services.

Overwriting
Overwriting is an approved method for the removal of City data from hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. The overwriting process including the software products and applications used for the overwriting process shall include the following steps:
a) The data shall be properly overwritten with pseudo random data by means of, at a minimum, one pass of the entire device for a 15 gigabyte or greater drive. A minimum of three passes of pseudo random data must be applied to drives smaller than 15 gigabytes in size.
b) The software shall have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any intelligible data.
c) The software shall have the capability to overwrite using a minimum of one pass or three passes of pseudo random data on all sectors, blocks, tracks, and any unused disk space on the entire disk medium.

d) The software or supporting software shall have a method to verify that all data has been removed. Verification must be performed to verify that each drive overwritten is, in fact, clean of any intelligible or prior data.
e) Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.

Degaussing

Degaussing is a process whereby the magnetic media is erased. Hard drives seldom can be used after degaussing. The degaussing method will only be used for hard drives when the drive is inoperable and will not be used for further service.
Please note that extreme care should be used when using degaussers since this equipment can cause damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. The following steps shall be followed when hard drives are degaussed:
a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.
b) Shielding materials (cabinets, mounting brackets), which may interfere with the degaussing equipment magnetic field, shall be removed from the hard drive before degaussing.
c) Hard disk platters shall be degaussed during the degaussing process in accordance with the manufacturer's specifications.

Physical Destruction

Hard drives shall be destroyed when they are at end of life, defective or cannot be repaired or City data cannot be removed for reuse.

a) Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.
b) Multiple holes drilled into the hard disk platters is an optional method of destruction that

b) Multiple holes drilled into the hard disk platters is an optional method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

Non-Volatile Memory Devices Data Removal Method

Electronic devices that hold data or configurations in non-volatile memory shall have all
City data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, fire-walls and switches.

Other Electronic Media Data Removal Methods

If there is any risk of disclosure of sensitive data on media other than hard drives or devices that hold data or configurations in non-volatile memory, that media should be overwritten, degaussed or destroyed. Disintegration, incineration, pulverization, shredding or melting is acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.
Flash drives may be overwritten with a three pass minimum. Diskettes, CDs, DVDs, Tape backups may be degaussed or destroyed. If overwriting or degaussing is selected, the steps for the selected method as stated in this standard shall be followed.

Burning, shredding or pulverizing of non-classified CD-ROMs by end- users is not recommended. CD-ROM discs do not require extensive destruction. Discs that are outdated or no longer needed may be rendered unreadable by cutting in half or deep scratching 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 to prevent unauthorized access to the data. These discs may be placed in the general waste stream for disposal.