Bedford County Tennessee

Digital Media and Hardware Disposal Policy

Date: 08.31.11
Approved By: Chris White
Policy Number: __________
## 1.0 INTRODUCTION

1.1 Authority
1.2 Purpose
1.3 Scope
1.4 Background

## 2.0 POLICY

2.1 Preface
2.2 Disposal Scenarios
2.3 Technical Guidance on Disposal
2.4 Compliance
2.5 Surplus Items
2.6 Copiers
2.7 Printers
2.8 Paper Based Media
2.9 Retention Period

## 3.0 POLICY NOTIFICATION

## 4.0 DEFINITIONS
1.0 Introduction

1.1 Authority

Authority given under The Bedford County Acceptable Use Policy for Electronic Equipment & Media Section 11.0. Managers, employees, records personnel, third party vendors and all others who connect to or handle Bedford County government networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that this policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

The purpose of this policy is to ensure the confidentiality and security of information about Bedford County government's employees, partners and citizens as well as any protected data and intellectual property and protect such data from unauthorized disclosure. Additionally, it can protect Bedford County government from potential breaches of software license agreements. It defines the disposal of digital media and hardware standards and procedures to be used by state agencies and departments.

1.3 Scope

This policy applies to all hardware, digital and paper based media owned, leased or produced by Bedford County government that is capable of storing or relaying personal information related to the privacy of its employees, partners and citizens as well as intellectual property or protected data. All vendors and contractors that do business on behalf of Bedford County government, who store confidential County information on their systems, shall also adhere to this policy. Storage devices include but are not limited to the following:

- Portable and notebook computers
- Copiers
- Printers
- Workstations
- Servers, routers and switches
- Mobile devices, such as PDA’s and smart phones
- Storage media such as hard drives, USB flash drives, external hard disks, floppy disks, optical CD and DVD media, magnetic tape and other long-term media
- Paper based Media
1.4 Background

As our society has become increasingly dependent on information systems, the risks associated with more sophisticated attacks to gain access to sensitive data has equally increased. The response to these attacks has been to institute a wide variety of deterrents designed to keep assailants at bay. As a result, attackers have started to use other methods to obtain sensitive data. One popular method is to recover residual data from discarded media devices. If data is recovered, this exposes the organization to potential negative consequences, including regulatory fines (e.g., HIPAA), punitive awards and loss of credibility with employees, partners and citizens, to name a few. Therefore, it is imperative that all Bedford County offices and departments follow a policy to ensure the protection of sensitive data both inside and outside the organization.

2.0 Policy

2.1 Preface

All equipment that may contain protected data, personal information or intellectual property must be processed as outlined in this policy prior to transfer for other uses or for disposal.

Agencies/departments shall develop procedures to outline the steps employees should follow for proper disposal of digital media and hardware, including transfer of equipment to IT. Proper chain of custody for all digital media must be followed.

If a device is to remain within a department, it may have less stringent requirements based on agency/department procedures. (See the Disposal Scenarios section of this policy.) Any device leaving a department must be processed according to this policy.

2.2 Disposal Scenarios

Categories for disposing of hardware and other forms of digital media as described above:

1. Hardware Transferred Internally

Hardware may not require the Department of Defense (DoD) standard of degaussing (seven overwrites), or hard drive destruction, when transferred to another user within the same department. (Department is defined as a specific area within Bedford County Government, i.e. I.T. is a department within the Bedford County Government.) Simple formatting or one wipe degaussing may be used for machines remaining within the same functional area of the department.
Departments may choose to use higher standards when dealing with more sensitive information or when the equipment is being redeployed in a different functional role within the same department. Hardware that is transferred to a different department must be processed as specified in the Hardware Transferred Externally section of this document.

2. Hardware Transferred Externally

All hardware transferred externally must be handled according to the methods defined in the Technical Guidance on Disposal section of this policy. Equipment, minus the digital media storage devices, will be handled by the Finance Department. Examples are, but not limited to:

- Hardware transferred to another department
- Hardware transferred to charitable organizations
- Hardware to be sold
- Hardware released to a third-party for disposal

2.3 Technical Guidance on Disposal

Two primary methods for disposal of digital media are:

1. Physical Destruction

Physical destruction will be the primary method used for the disposal of digital media and data storage devices contained in equipment that will be redeployed outside of an agency/department.

Digital media may be disposed of by disintegration, incineration, shredding, crushing, or pulverizing. All computing and communication equipment leaving a department or agency for disposal will have the digital media (hard drive, tapes, disks, etc.) pulled by the IT department prior to any disposal method. The digital media devices are to be locked in a secure area until they are destroyed.

2. Digital Degaussing

Digital degaussing will be used when equipment is being redeployed (see above) or in cases of “exception” when physical destruction is not reasonable or is prohibitive.

Deleting files is insufficient to certify that sensitive information cannot be recovered from the digital media drives. Departments must ensure that deletion is complete through the use of specialized tools that meet federal guidelines and standards, or through contractual relationships with vendors who use equipment that can meet these standards or through the county’s IT department. Therefore, a digital degaussing tool must be used. The tool must conform to the Department of Defense’s DoD 5220.22-M specifications, available at:

http://www.dtic.mil/whs/directives/corres/html/522022m.htm

Exception: Servers, routers, switches and other hardware that are under warrantee, and which are sent back for service or repair, should have IP addresses and configuration information scrubbed prior to return to the company. Also, this equipment should be delivered in a fashion that results in a signed verification of receipt by the company. The county IT office or the department’s IT division (if applicable) is responsible for having a written procedure for this process.

2.4 Compliance

Compliance with this policy is mandatory.

Each department is responsible for establishing procedures to implement this policy. Any agency not adhering to this policy may potentially expose itself to legal ramifications and regulatory fines to include possible punitive damages. Employees must be notified of the procedures to decommission IT computing and communication equipment and the proper disposal of storage media external to the equipment.

2.5 Surplus Items

Equipment such as keyboards, mice, monitors, towers, laptops etc. that are decommissioned (excluding the data storage devices such as hard drives) will be sent to the Finance Department for processing, storage, recycling to other departments or listing on Gov.deals.com.

2.6 Copiers

If a copier is being moved/removed from a department or building, it is the responsibility of the appropriate contracted vendor to remove the hard drive prior to moving the machine. Once the hard drive is removed from the machine, the copier may be removed from the area. The hard drive will be handled as described in the policy.

2.7 Printers

All printers must be purchased/leased through Finance Department purchasing and contracting processes. The use of personally owned printers is prohibited.

Printers will be removed by the contracted hardware disposal vendor or IT department to be disposed of per this policy.

2.8 Paper Based Media

Any paper-based or other hard copy media containing confidential data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the County for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5mm (1/32”x1/5”). Media
containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the department, county government operations, employees or affiliate organizations.

Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

2.9 Retention Period

Departments should retain copies of their digital media and hardware destruction receipt forms for a three (3) year period.

3.0 Policy Notification

Each department is responsible for ensuring that employees are aware of where policies are located on websites or in physical form. Departments are also responsible for notifying employees of policy change or the creation of new policies that pertain to the department function.

4.0 DEFINITIONS

1. DeGaussing – Demagnetizing magnetic storage media such as tapes or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.
2. Disintegration – A physically destructive method of sanitizing data; the act of separating into component parts.
4. Incineration – A physically destructive method of sanitizing media; the act of burning completely to ashes.
5. Internal Data – County Government Data intended for internal government business only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need.
6. **Media** – Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CD’s and DVD’s, or paper-based products.

7. **Media Sanitation** – The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

8. **Pulverization** – A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

9. **Purging** – A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting, exceeds the value of the data to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.