

State of Vermont

Digital Media and Hardware Disposal Standard



Date: June 26, 2009

Approved by: Neale F. Lunderville, Secretary of Administration

Policy Number:

1.0 INTRODUCTION..... 3

 1.1 Authority..... 3

 1.2 Scope and Purpose:..... 3

2.0 STANDARD 3

 2.1 Preface..... 3

 2.2 Chain of Custody..... 4

 2.2.1 Chain of Custody for Media Destruction..... 4

 2.2.2 Chain of Custody for Shells and Peripherals..... 5

 2.3 Disposal Requirements 6

 2.4 Documentation..... 6

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), "to provide direction and oversight for all activities directly related to information technology and security in state government."

The National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, "Recommended Security controls for Federal Information Systems," specifies that, "The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media." *Title 29: Public Property and Supplies, Chapter 59, § 1552. Authority and duties*, states that the department of Building and General Services (BGS) is responsible for the disposal of all State owned property.

1.2 Scope and Purpose:

To establish the requirements for proper disposal of all hardware and digital media owned or leased by the State of Vermont that is capable of storing intellectual property, protected data, or personal information related to the privacy of its employees, partners and citizens.

2.0 Standard

2.1 Preface

Disposing of computers without ensuring proper file deletion presents huge business risks as well as the danger of non-compliance with federal laws including the Gramm-Leach Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA).

A contracted vendor will be responsible for the destruction of all hard drives, tapes, or other digital media devices. The only exceptions are a machine or device being transferred to another user within a department or if a device is under warranty and is to be returned to the vendor. (See Hardware Sanitization Policy 2.2.)

The contracted vendor's employees will have background checks to the level of FBI standards for security requirements.

Buildings and General Services (BGS) will be the central contact for collection of all IT equipment that will be redeployed. The exception to this standard is hardware that is transferred within the same department or hardware that is unwanted by BGS. In this case, the agency/department IT personnel may wipe the hard drive as deemed appropriate by the IT department, department supervisor or his/her designee. Hardware that is not returned to BGS will be picked up by the contracted vendor for recycling.

2.2 Chain of Custody

It is critical that hardware and digital media be tracked from its point of origin within an agency/department through the disposal process. Loss of data can result in expensive investigations, loss of credibility, as well as possible litigation.

The Chain of Custody form (see Appendix A) must be filled out for media to be destroyed as well as IT equipment to be recycled through BGS or a contracted vendor.

2.2.1 Chain of Custody for Media Destruction

The state contracted vendor will destroy digital media storage devices. Such devices are contained within, but are not limited to the following:

- Portable and notebook computers
 - Desk top computers
 - Hand held wireless devices. (Smart phones should be returned to the agency IT department when no longer in use. The IT department will determine whether the device can be redeployed after degaussing or be destroyed.)
 - Removable storage devices such as flash drives, floppy disks, optical CD and DVD media, tape and other long-term storage devices.
1. Department/agency IT representative will pull the hard drives, tapes or other forms of digital media from the machine(s).
 2. Complete the "Hardware Chain of Custody" form noting the serial number of each hard drive or tape. If a device, such as a tape, does not have a serial

number, a unique number will be assigned to the device for inventory and tracking purposes.

3. The digital media will be stored in a locked, secure area.
4. The IT department employee will contact the contracted vendor to come and destroy the hard drives or other media at the site or securely transport the media to their facility for destruction.
5. The contracted vendor will supply a copy of the serial numbers of the hard devices destroyed and a certificate of destruction to an appointed individual within the IT department. This document must be compared to the Chain of Custody form and confirmed that all media has been destroyed.
6. Records must be maintained for three years per DoD Standards.

2.2.2 Chain of Custody for Shells and Peripherals

The Department of Buildings and General Services (BGS) will be responsible for deciding the disposition of the shells, peripherals and other IT equipment, except for cell phones (see above). Shells designed for Windows XP or higher will be returned to BGS (without hard drives). All other shells and hardware will be removed by the contracted vendor for recycling. This includes, but is not limited to the computer shells, keyboards, mouse, monitors and other peripherals.

Agencies are responsible for all costs associated with the recycling or destruction of hardware by the contracted media disposal vendor.

A Chain of Custody form(s) must be completed to reflect the hardware being sent to BGS. The department employee responsible for handing off the hardware will confirm with the BGS driver (for computer shells and peripherals) that the inventory documented on the form(s) match the hardware to be taken to BGS.

- a. Both the department employee and driver will sign the form to confirm that the information on the form is correct and complete.
- b. One copy of the form will stay with the department and the original will go with the driver. The agency/department will keep a record for three years per DoD standards.
- c. BGS or a contracted vendor will pick up hardware at agency sites as needed.
- d. The driver will pick up all hardware listed on the "Hardware Chain of Custody" form. If there is additional equipment to be moved, an additional form will need to be completed to account for the additional equipment. No hardware will be picked up without being accounted for.

- e. When the hardware is delivered to BGS, a BGS employee and the driver will verify that all hardware delivered matches the list provided by the agency/department.

2.3 Disposal Requirements

1. A contracted vendor will be responsible for the destruction of all digital media. The method of destruction of hard drives will employ a pneumatic hammer. This method of destruction meets all Department of Defense (DoD) and National Institute of Standards and Technology (NIST) requirements. Other types of media, not able to be destroyed by the pneumatic hammer, will be destroyed at the contracted vendor's facility. (All contracted vendor employees have FBI level background checks, the trucks are locked at all times.) Chain of Custody form(s) are required prior to any destruction or removal of digital media.
2. If there is a case where a device should be wiped rather than destroyed, a degassing product will be used by the contracted vendor that meets with NIST and DoD degaussing standards.
3. The standard, DoD 5220.22-M requires "that storage contain no residual data from the previously contained object before being assigned, allocated, or reallocated to another user. Specifically, the DoD 5220.22-M standard requires overwriting with a pattern, then its complement and finally, with another pattern of 1's and 0's. DoD compliance requires 1's and 0's written across every track and sector seven times. All hardware sanitization will require seven wipes to meet the maximum requirements of the DoD.

2.4 Documentation

BGS will be responsible for maintaining documentation of the following:

- ✓ Chain of Custody forms upon receipt of hardware from agencies/ departments.
- ✓ Disposition of hardware.

Agencies will be responsible for maintaining documentation of the following:

- ✓ Chain of Custody forms for digital medial destruction with the contracted vendor.
- ✓ Certifications of destruction.
- ✓ Chain of Custody forms for equipment sent to BGS or to the contracted vendor.

All documentation will be retained for three years per DoD Standard DOD 5220.22-M.

Approved by:

Secretary of Administration:



Neale F. Lunderville

Date:

6/26/09