# State of Vermont

## Digital Media and Hardware Disposal Policy

Date: June 26, 2009
Approved by: Neale F. Lunderville, Secretary of Administration
Policy Number:

# 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."

## 1.2 Purpose

The purpose of this policy is to ensure the confidentiality and security of information about the State of Vermont's employees, partners and citizens as well as any protected data and intellectual property. 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 and digital media owned or leased by the State of Vermont that is capable of storing 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 the state, who store confidential state information on their systems, shall also adhere to this policy. Storage devices include, but are not limited to the following:

- Portable and notebook computers
- Workstations
- Servers, routers and switches
- Mobile devices, such as PDA's and smart phones
- Removable storage media such as flash drives, external hard disks, floppy disks, optical CD and DVD media, tape and other long-term storage 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 State agencies 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. (A sample *Chain of Custody* form is provided in Appendix A.)

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. (See Digital Media and Hardware Disposal Standard provided in Appendix B.)

## 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 an agency, i.e. DII is a department within the Agency of Administration.) Simple formatting or one wipe degaussing may be used for machines remaining within the same functional area of the department. (Example: The networking functional area, within DII, may exchange machines among networking staff. However, networking machines may not be assigned to the project management staff, within DII, without first being degaussed.) Agencies/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 department. Hardware that is transferred to a different department/agency 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 Buildings and General Services (BGS). Examples are, but not limited to:

- Hardware transferred to another agency
- 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 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. Agencies/departments will call a contracted vendor to pick up and destroy the digital media devices. (See the Digital Media and Hardware Disposal Standard provided in Appendix B.)

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 devices. Agencies/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. 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

In addition, degaussing methods must follow the recommendations outlined in the National Institute of Standards and Technology's Special Publication 800-88 – *Guidelines for Media Sanitization*, available at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

Exception: Servers, routers, switches and other hardware that are under warrantee should have IP addresses, 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. Each agency IT department is responsible for having a written procedure for this process.

## 2.4 Compliance

Compliance with this policy is mandatory.

Each agency 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

*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. Equipment such as keyboards, mice, monitors, towers, laptops etc. that are decommissioned (minus the data storage devices such as hard drives) will be sent to BGS unless BGS specifically indicates that the equipment is to be recycled by the agency/department. In the case of recycling, a contracted vendor will pick up the equipment from the agency/department.

## 2.6 Training

Each State agency is responsible for ensuring that its employees are properly trained in accordance with this policy and any related internal agency policies and procedures.

## 2.7 Retention Period

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

Approved by:

Secretary of Administration: Neale F. Lunderville

Neale F. Lunderville

Date: 6/26/09