

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	05-01				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Media Handling & Security		

1 Policy Statement:

State Agency data storage devices and printed media shall be disposed of in a manner consistent with the security categorization of the information contained on these devices or media.

1.2 Policy Objective:

Ensure the secure disposition of physical and electronic information along with the hardware and electronic media on which it is stored.

1.3 Policy and Control Requirements:

Compliant Activities.

- All data and programs shall be removed from electronic storage media by State Agencies before sending the storage media to RI Division of IT, Surplus Division (State Surplus) moving to another agency, exchanging with a vendor while under warranty, donating, and/or destroying.
- State Agencies shall maintain a log that provides an audit trail of destruction or disposition of the device.
- The method used for removal of data depends upon the operability of the device.
- 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, it shall be physically destroyed or degaussed.
- If the hard drive is inoperable, has reached the end of its useful life, or cannot be properly overwritten, then it shall be physically destroyed or degaussed.
- Acceptable methods of removing data are: overwriting, degaussing, and physical destruction.

Overwriting

- When overwriting data, it shall be properly overwritten with a pattern that complies with
 - the Department of Defense (DOD) standard 5220.22-M, or
 - the Department of Defense (DOD) standard 5200.28-STD, or
 - Peter Gutmann 35-pass wiping scheme.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	05-01				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Media Handling & Security		

- Removal of state data is not considered complete until at least three overwrite passes and a full verification pass have been completed.
- The software used shall have the capability to overwrite the entire disk drive, independent of any Basic Input/Output System (BIOS) or firmware capacity limitation, making it impossible to recover any meaningful data.
- The software shall have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.
- The software shall have a method to verify that all data has been removed.
- Sectors not overwritten shall be identified.

Degaussing.

- When degaussing any media, the product manufacturer's directions shall be carefully followed. It is essential to determine the appropriate rate of coercivity (magnetic saturation) for degaussing.
- Shielding materials (cabinets, mounting brackets) that may interfere with the degausser's magnetic field shall be removed from the hard drive before degaussing.
- Hard disk platters shall be in a horizontal direction during the degaussing process.

Physical Destruction

- Hard drives shall be destroyed when they are defective, cannot be repaired, or when State data cannot be removed for reuse.
- Physical destruction shall be accomplished to an extent that precludes any possible further use of the hard drive. This can be achieved by removing the hard drive from the cabinet, removing any steel shielding materials and/or mounting brackets, and cutting the electrical connection to the hard drive unit. The hard drive shall 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.
- Drilling multiple holes into the hard disk platters is another method of destruction that will preclude use of the hard drive and provide *reasonable* protection against unauthorized retrieval of the data written on the drive.

Removal of State Data/Programs from Other Electronic Devices.

- Electronic devices that hold user data or configurations in volatile memory shall have all State data removed by either the removal of the battery or electricity supporting the

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	05-01		2/15/07	3/2/06	3 of 5
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Media Handling & Security		

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, Personal Digital Assistants (PDA), routers, firewalls and switches.

Removal of State Data/Programs from Other Computer Media.

- If there is any risk of disclosure of confidential or sensitive data on media other than computer hard drives, that media shall be destroyed. Disintegration, incineration, pulverization, shredding, or melting is an acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, Write Once/Read Many (WORM) devices, and Universal Serial Bus (USB) data storage devices.

Certification of the Removal of State Data/Programs from Surplus Computer Hard Drives and Electronic Media.

- Each State Agency shall establish and use an audit procedure to ensure compliance with standards.
- Prior to submitting surplus forms to the agency's appropriate organizational unit, the process for removal of State data shall be documented on a form or file that explicitly outlines:
- The methods (**Overwrite, Degauss, and Destruction**) used to expunge the data from the storage media.
- The make and model of equipment that was released for surplus from which State data was removed.
- The state inventory ID.
- The serial number of the personal computer or other equipment.
- The name of the person responsible for the removal of state data.

The completed form/file (containing the following information) shall be maintained in a central location, by each State Agency, for audit purposes.

Method of Sanitation	Make and Model of Equipment	State ID Number	Serial Number	Name of Person Who Performed the Sanitation/Destruction

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	05-01				
State of Rhode Island Department of Administration Division of Information Technology	TITLE	Media Handling & Security			

When sending equipment to State Surplus, a label shall be affixed to the equipment to denote that the information has been removed.

See the sample label below.

Storage media has been sanitized per IOT media destruction policy Date ____ / ____ / ____ Technician:
--

- The disposal of storage media without removal of the data with an approved method.
- Deleting files does not normally remove information from storage media.

Since the delete process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing state data from State Agency-owned hard disks or other storage media.

1.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the State CSO or the CSO's designee.

1.5 Policy Violations and Disciplinary Actions:

An employee found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

1.6 Implementation Responsibility:

RI DOIT shall establish and maintain guidance regarding acceptable methods for destruction of media and removal of data.

Each State Agency is responsible for auditing the removal of State data for compliance with this standard when any computer hard drive or electronic media are released for surplus, transferred, traded in, disposed of, or the hard drive is being replaced. The State

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	05-01				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Media Handling & Security		

Agency shall ensure that the audit process occurs in a timely manner, and that the audit controls are effective.

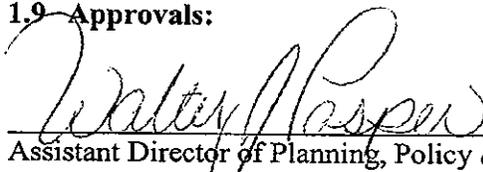
1.7 Compliance Responsibility:

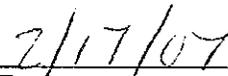
The RI DOIT and State Agencies shall be responsible for implementing and enforcing the Media and Data Destruction Policy within their supported areas.

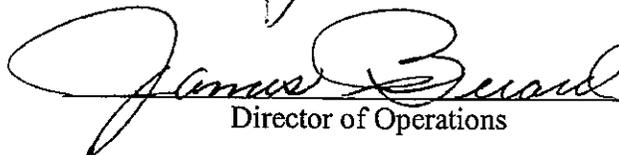
1.8 References:

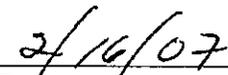
- Department of Defense (DOD) standard 5220.22-M
- Department of Defense (DOD) standard 5200.28-STD
- Peter Gutmann 35-pass Wiping Scheme
- HIPAA 164.310 (d) (1) Device and Media Controls
 - (2) Implementation Specifications
 - (i) Disposal
 - (ii) Media Reuse
 - (iii) Accountability

1.9 Approvals:

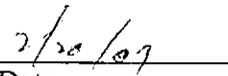

 Assistant Director of Planning, Policy & Technology


 Date


 Director of Operations


 Date


 Chief Information Officer


 Date

 Director, Department of Administration

 Date