NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 152-01 – Information Disposal and Media Sanitization Standard	**POLICY NO:** 09-10-S1-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 04/08/2011
	VERSION: 2.0	**LAST REVIEWED:** 01/22/2015

ATTN: Directors of Administration and Agency IT Directors

1 PURPOSE

This standard is to ensure the proper disposal and/or sanitization will be conducted of media that has been damaged, is being repurposed, and/or has reached the end of its life. This standard establishes a media clear, purge and/or destroy process based on the classification of the information contained on the media according to the **NIST SPECIAL PUBLICATION 800-88 GUIDELINES FOR MEDIA SANITIZATION**.

2 AUTHORITY

This circular is established under the authority of State of New Jersey **N.J.S.A. 52:18A-230 B**. This order defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch of State Government.

The Office of Information Technology (OIT) reserves the right to change or amend this circular.

3 SCOPE

This procedure applies to all personnel including employees, temporary workers, volunteers, contractors, and those employed by contracting entities, and others who are responsible for the disposal, sanitization, and destruction of the State of New Jersey property.

4 RESPONSIBILITIES

Administrative Directors working in conjunction with the agency IT Directors shall be responsible for ensuring the effective implementation of statewide information technology circulars.

5 STANDARD

This standard will address information security processes pertaining to media disposal and sanitization in accordance with the NIST Special Publication 800-88 Guidelines for Media Sanitization document. The information security concern regarding media disposal and sanitization reside not in the media itself but in the recorded or stored information on the media. The disposal and sanitization of media is driven by the classification of the information placed intentionally or unintentionally on the media.

In the absence of a classification, media shall, by default, be given the highest level of classification to ensure proper media disposal. This is to confirm that residual magnetic, optical, electrical, or other representation of data has been removed from stored media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

The different processes of sanitization for each type of media are provided in the attached *Appendix A – Media Sanitization*. Departments and Agencies must categorize their data, assess the nature of the medium on which it is stored, assess the risk to security and/or confidentiality, and determine the type of sanitization method that is appropriate for the media.

Departments and Agencies must ensure that suitable business processes meet or exceed the NIST Special Publication 800-88 Guidelines when disposing of or sanitizing media. This process must be implemented in such a manner to ensure that all State data is properly sanitized from said media for administrative, maintenance, or repair purposes.

Departments and Agencies must ensure that service provider who repairs media that fail while covered by the manufacturer warranty, use an approved method of destruction for the proper sanitization of the media and request appropriate documentation/certification of the sanitization process from the responding vendor.

An inventory record of all repurposed, repaired, and disposed of hardware must be kept by all Departments and Agencies.

6 EXCEPTIONS AND NON-COMPLIANCE

Departments and agencies shall comply with this policy within 90 days of its effective date.

Failure to comply with this policy may result in disciplinary action. Requests for exceptions for non-compliance with this policy shall be processed in accordance with Circular 08-02-NJOIT, *111 – Information Security Managing Exceptions*.

Media Sanitization

Media Type	Clear	Purge	Physical Destruction
Hard Copy Storages			
Paper and microforms	See Physical Destruction.	See Physical Destruction.	• Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL.). • Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.
Hand-Held Devices			
Cell Phones	Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	• Shred • Disintegrate • Pulverize. • Incinerate by burning cell phones in a licensed incinerator.
Personal Digital Assistant (PDA) (Palm, Pocket PC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	• Incinerate PDAs by burning the PDAs in a licensed incinerator. • Shred • Pulverize

Networking Devices			
Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	• Shred • Disintegrate • Pulverize • Incinerate routers by burning the routers in a licensed incinerator.
Equipment			
Copy Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	• Shred • Disintegrate • Pulverize • Incinerate copy machines by burning the copy machines in a licensed incinerator.
Fax Machines	Perform a full manufacturer's reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.	Same as Clear.	• Shred • Disintegrate • Pulverize • Incinerate fax machines by burning the fax machines in a licensed incinerator.
Magnetic Disks			
Floppies	Overwrite media by using Statewide Office of Information Security-approved software and validate the overwritten data.		• Incinerate
ATA Hard Drives	Overwrite media by using Statewide Office of Information Security-approved and validated overwriting technologies/methods/tools.	Purge media by using Statewide Office of Information Security-approved and validated purge technologies/tools. a. Active KillDisk Professional b. GEEP EDS EBAN	• Disintegrate • Shred • Pulverize

	See Purging	c. Secure Erase	• Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	Overwrite media by using Statewide Office of Information Security approved and validated overwriting technologies/methods/tools. See Purging	Purge media by using Statewide Office of Information Security-approved and validated purge technologies/tools. a. Active KillDisk Professional b. GEEP EDS EBAN c. Secure Erase	• Disintegrate • Shred • Pulverize • Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator
Zip Disks	Overwrite media by using Statewide Office of Information Security-approved and validated overwriting technologies/methods/tools. See Purging	Purge media by using Statewide Office of Information Security-approved and validated purge technologies/tools. a. Active KillDisk Professional b. GEEP EDS EBAN c. Secure Erase	• Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. • Shred
SCSI Drives	Overwrite media by using Statewide Office of Information Security-approved and validated overwriting technologies/methods/tools. See Purging	Purge media by using Statewide Office of Information Security-approved and validated purge technologies/tools. a. Active KillDisk Professional b. GEEP EDS EBAN c. Secure Erase	• Disintegrate • Shred • Pulverize • Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Magnetic Tapes			
Reel and Cassette Format Magnetic Tapes	1. Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.	Degauss using an NSA/CSS-approved degausser. Reference Appendix C – NSA Evaluated Products List - Degausser. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be	• Incinerate by burning the tapes in a licensed incinerator. • Shred • Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may

	2. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.	accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.	be necessary to comply with the requirements of a destruction facility or for recycling measures.
Optical Disks			
CDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of recommendations: • Removing the Information bearing layers of CD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm^2.
DVDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of recommendations: • Removing the Information bearing layers of DVD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility.

			• Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.
Memory			
Compact Flash Drives, SD	Overwrite media by using Statewide Office of Information Security--approved and validated overwriting technologies/methods/tools.	See Physical Destruction.	Destroy media in order of recommendations. • Shred • Disintegrate • Pulverize • Incinerate by burning in a licensed incinerator
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	• Shred • Disintegrate • Pulverize
Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's data sheets.	Same as Clear.	• Shred • Disintegrate • Pulverize
Electronically Erasable PROM (EEPROM)	Overwrite media by using Statewide Office of Information Security- approved and validated overwriting technologies/methods/tools. Remove all labels or markings that indicate previous use or confidentiality.	Same as Clear.	• Shred • Disintegrate • Pulverize • Incinerate by burning in a licensed incinerator.

Erasable Programmable ROM (EPROM)	Clear media in order of recommendations. 1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time requirement by a factor of 3. 2. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Same as Clear.	• Shred • Disintegrate • Pulverize • Incinerate by burning in a licensed incinerator.
Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	Overwrite media by using the Statewide Office of Information Security--approved and validated overwriting technologies/methods/tools.	Same as Clear.	• Shred • Disintegrate • Pulverize
Field Programmable Gate Array (FPGA) Devices (Volatile)	Clear functioning FPGA by powering off and removing the battery (if battery backed).	Same as Clear.	• Shred • Disintegrate • Pulverize
Flash Cards	Overwrite media by using the Statewide Office of Information Security- approved and validated overwriting technologies/methods/tools.	Same as Clear.	• Shred • Disintegrate • Pulverize
Flash EPROM (FEPROM)	Perform a full chip purge as per manufacturer's data sheets.	Purge media in order of recommendations. **A.** Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Perform a full chip purge as per manufacturer's data sheets.	• Shred • Disintegrate • Pulverize • Incinerate by burning in a licensed incinerator.

Magnetic Bubble Memory	Overwrite media by using the Statewide Office of Information Security-approved and validated overwriting technologies/methods/tools.	Purge by Collapsing the Magnetic Bubbles: 1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing. Reference Appendix C – NSA Evaluated Products List - Degausser. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure.	• Shred • Disintegrate • Pulverize • When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Magnetic Core Memory	Clear media in order of recommendations. 1. Overwrite media by using Statewide Office of Information Security-- approved and validated overwriting technologies/methods/tools. 2. Degauss in an NSA/CSS-approved degausser. Reference Appendix C – NSA Evaluated Products List - Degausser.	Purge core memory devices by either overwriting or degaussing. • Overwrite media by using Statewide Office of Information Security-approved and validated overwriting technologies/methods/ tools • Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure performance and should be	• Shred • Disintegrate • Pulverize • When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance.

		considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing. Reference Appendix C – NSA Evaluated Products List - Degausser.	
Non Volatile RAM (NOVRAM)	1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Each overwrite must reside in memory for a period longer than the data resided. 3. Remove all power to include battery power.	Same as Clear.	• Shred • Disintegrate • Pulverize
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator.
RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	• Shred • Disintegrate • Pulverize

ROM	See Physical Destruction.	See Physical Destruction.	• Shred • Disintegrate • Pulverize
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using agency approved and validated overwriting technologies/methods/tools.	Same as Clear.	• Shred • Disintegrate • Pulverize
Smart Cards	See Physical Destruction.	See Physical Destruction.	• For smart card devices& data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles.
Magnetic Cards			
Magnetic Cards	See Physical Destruction.	See Physical Destruction.	• Shred • Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator.

Type	Description
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
Clearing	Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method. [SP 800-36]. Studies have shown that most of today's media can be effectively cleared by one overwrite. Specific recommendations for clearing different media types are included in Appendix A.
Purging	Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed. Specific recommendations for purging different media types are included in Appendix A. If purging media is not a reasonable sanitization method for organizations, this guide recommends that the media be destroyed.

Destroying	Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack. • *Disintegration, Incineration, Pulverization, and Melting*. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shredding*. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, and CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

NSA EVALUATED PRODUCTS LIST – DEGAUSSER

ELECTROMAGNETIC DEGAUSSER EQUIPMENT

Drawer Type Degaussers: These are electromagnetic degaussers that provide automatic one pass operation for tape storage device erasure. Models certified for disk storage device erasure can be used to erase disks 3.5" or smaller. The disk must be placed horizontally, degaussed once, turned over and degaussed a second time. All extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, must be removed before degaussing. The degaussers must be operated at their full magnetic field strength. The erasure of hard disk drives causes damage that prohibits their continued use.

NOTE: ADAPTORS MAY BE NECESSARY TO ACCOMMODATE THE VARIOUS SIZES OF STORAGE DEVICE PRODUCTS.

MANUFACTURER	MODEL	TAPE (Oe)	DISK (Oe)
Data Devices International 2600 Mission Street San Marino, CA 91108-1676 626.799.6545 ATTN: David Partridge	Cambrian	350	Not Tested
Data Security, Incorporated 729 Q Street Lincoln, NE 68508 402.434.5959 800.225.7554 www.datasecurityinc.com ATTN: Renee Schafer rschafer@telesis-inc.com	Type I, 911-0000	350	Not Tested
Data Security, Incorporated	Type HD-2000, 940-0001	750	L-1500
Data Security, Incorporated	Type HD-2000, 940-0001	750	L-1800
Garner Products 620 Commerce Drive Suite C Roseville, CA 95678 800.624.1903	CF750	750	Not Tested
Data Security, Incorporated	Type II-A, 930-0000	1000	Not Tested
Data Security, Incorporated	Type III, 943-0001	1700	Not Tested

MANUFACTURER	MODEL	TAPE (Oe)	DISK (Oe)
Conveyor Type Degaussers: These are electromagnetic degaussers that are continuous duty conveyor belt types and provide one pass erasure for tape storage devices.			
Garner Products 620 Commerce Drive Suite C Roseville, CA 95678 800.624.1903	2700	350	Not Tested
Chamber Type Degaussers: These are electromagnetic degaussers that provide automatic one pass operation for disk and tape storage device erasure. They can be used to erase disks 3.5" or smaller. All extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, must be removed before degaussing. The degaussers must be operated at their full magnetic field strength. The erasure of hard disk drives causes damage that prohibits their continued use.			
Data Security, Incorporated 729 Q Street Lincoln, NE 68508 402.434.5959 800.225.7554 www.datasecurityinc.com ATTN: Renee Schafer rschafer@telesis-inc.com	HD-6600	2800	L-4200
Data Security, Incorporated	HD-1T	2800	L-5000 P-5000
Proton Engineering Inc. P.O. Box 1852 P-5000 Palm City, Florida 34991 772.223.1685 ATTN: William Olliges proton@bellsouth.net	T-4	2800	L-5000
Security Engineered Machinery 4420-B Lottsford Vista Road Lanham, MD 20706 800.645.1157 301.735.7100 ATTN: Terry Creek	EMP 001 Eliminator	2800	L-5000 P-5000

PERMANENT MAGNET DEGAUSSER EQUIPMENT

Hand Degaussers: These are hand held permanent magnet degaussers. To degauss disk storage devices, insert the degaussing wand into the disk pack so that the active magnetic portion completely covers the recording surface of the disk from hub to perimeter. Wipe each active disk surface (top and bottom) at least three times with the magnet. If disks are part of a sealed hard disk drive assembly, they must be removed from the assembly for degaussing. The erasure of hard disk drives causes damage that prohibits their continued use.

MANUFACTURER	MODEL	TAPE (Oe)	DISK (Oe)
Applied Magnetics Laboratory, Inc. 1404 Bare Hills Rd. Baltimore, MD 21209 410.583.2100	AML-6KG	Not Tested	L-5000
Proton Engineering, Inc P.O. 1852 Palm City, Florida 34991 772.223.1685 ATTN: William Olliges proton@bellsouth.net	1100	Not Tested	L-5000
Whitaker Brothers Business Machines, Inc. 12410 Washington Avenue Rockville, MD 20852 800.243.9226 301.230.2800 www.whitakerbrothers.com ATTN: Vivian Kambanis gsa@whitakerbrothers.com	102-DG	Not Tested	L-5000
Single Pass Slot Degaussers: These are enclosed permanent magnet degaussers that require one pass for proper erasure. The erasure of hard disk drives causes damage that prohibits their continued use.			
Applied Magnetics Laboratory, Inc 1404 Bare Hills Rd. Baltimore, MD 21209 410.583.2100	Magnastroyer AML-MS1	2150	L-750
Dual Pass Slot Degaussers: These are enclosed permanent magnet degaussers. To properly degauss disk storage devices, pass the disk through the entry slot, turn the disk 90 degrees and slide the disk through the slot again. The erasure of hard disk drives causes damage that prohibits their continued use.			

MANUFACTURER	MODEL	TAPE (Oe)	DISK (Oe)
Proton Engineering, Inc. P.O. Box 1852 Palm City, Florida 34991 772.223.1685 ATTN: William Olliges proton@bellsouth.net	1090	Not Tested	L-750
Drawer Degaussers: These are enclosed permanent magnet degaussers that provide automatic one pass operation for disk and tape storage device erasure. All extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, must be removed before degaussing. The erasure of hard disk drives causes damage that prohibits their continued use.			
Data Security, Incorporated 729 Q Street P-5000 Lincoln, NE 68508 402.434.5959 800.225.7554 www.datasecurityinc.com ATTN: Renee Schafer rschafer@telesis-inc.com	APM-10	2800	L-5000 P-5000
Data Security, Incorporated	HPM-1	2800	L-5000 P-5000
Data Security, Incorporated	HPM-1A	2800	L-5000 P-5000
Data Security, Incorporated	HPM-4	2800	L-5000 P-5000
Data Security, Incorporated	HPM-4E	Not Tested	L-5000 P-5000
Garner Products 620 Commerce Drive Suite C Roseville, CA 95678 800.624.1903 Red River Computer ME-RRC3 2800 L-5000 85 Mechanic Street P-5000 Lebanon, NH 03766 603.448.8880 www.redriver.com ATTN: Kurt Gantrish	REM-1400NSA	2800	L-5000 P-5000
Red River Computer	ME-RRC3M	2800	L-5000 P-5000

MANUFACTURER	MODEL	TAPE (Oe)	DISK (Oe)
Security Engineered Machinery/ Toshiba 4420-B Lottsford Vista Road Lanham, MD 20706 800.645.1157 301.735.7100 ATTN: Terry Creek	ME-P3	2800	L-5000 P-5000
Security Engineered Machinery/ Toshiba	ME-P3E	2800	L-5000 P-5000
Security Engineered Machinery/ Toshiba	ME-P3M	2800	L-5000 P-5000
Conveyor Type Degaussers: These are enclosed permanent magnet degaussers that are continuous duty conveyor belt types and provide one pass erasure for disk and tape storage devices. All extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, must be removed before degaussing. The erasure of hard disk drives causes damage that prohibits their continued use.			
Data Security, Incorporated 729 Q Street Lincoln, NE 68508 402.434.5959 800.225.7554 www.datasecurityinc.com ATTN: Renee Schafer rschafer@telesis-inc.com	LM-4	2800	L-5000 P-5000
Data Security, Incorporated	LM-4E	Not Tested	L-5000 P-5000
Dexter Magnetic Technologies 400 Karin Lane Hicksville, NY 11801 908.668.4821 ATTN: Thomas Devaney	U5000	2800	L-5000 P-5000
Data Security, Incorporated 729 Q Street Lincoln, NE 68508 402.434.5959 800.225.7554 www.datasecurityinc.com ATTN: Renee Schafer rschafer@telesis-inc.com	Field CheckR		