

North Shore–LIJ Health System, Inc.

| | |
|---|---|
| POLICY TITLE: Equipment Disposal Policy and Procedure | ADMINISTRATIVE POLICY AND PROCEDURE MANUAL |
| POLICY #: 900.29 | CATEGORY: Information Services |
| System Approval Date: 12/12/13 | Effective Date: Internally 1/2006 |
| Site Implementation Date: | Last Revised/Reviewed: |
| Prepared by: Office of the CIO–IS Policy and Procedure Committee | Superseded Policy(s)/#: n/a |

GENERAL STATEMENT OF PURPOSE

The primary purpose for this policy is to securely and lawfully dispose of North Shore-LIJ Health System’s (“Health System”) IT equipment and Portable Storage Devices in compliance with applicable federal, state and local laws, regulations, and standards (e.g. HIPAA and PCI-DSS). Following these procedures, will minimize the risk of the inadvertent disclosure of *Sensitive and Highly Sensitive* information such as Protected Health Information (PHI), card holder data, and Personally Identifiable Information (PII) at the end of the equipment lifecycle. These Standard Operating Procedures are provided to support the *Device and Media Control Policy* 900.26.

POLICY

It is policy of the Health System to maintain the confidentiality of our data no matter where that data may reside. This document establishes the procedures for the lawful, efficient disposal of information technology equipment and Portable Storage Devices at Health System to ensure the ongoing protection and confidentiality of *Sensitive and Highly Sensitive* data.

SCOPE

This policy applies to all members of the North Shore-LIJ Health System workforce including, but not limited to, employees, medical staff, volunteers, students, physician office staff, and other persons performing work for or at North Shore-LIJ Health System.

DEFINITIONS

Disposal Administrator: The vendor engaged to administer the disposal of technology on behalf of the Health System.

Disposal Vendor: The vendor engaged by the Disposal Administrator to dispose of the technology.

Computer Clean Out (CCO): The program for the direct removal, sale and disposal of computer equipment from Health System locations.

Portable Storage Device: Any device used to transfer data in, out, or within the Health System network. This includes, but is not limited to:

- flash drives, thumb drives, etc.
- mp3 players (in data mode)
- Smartphones – Tablets
- Backup tapes and related media
- USB portable drives
- PDAs
- CDs and DVDs
- SD cards and other removable memory cards

PROCEDURE/GUIDELINES

This Standard Operating Procedure covers three main categories of equipment: portable storage devices, leased equipment, and computers. The computers category is addressed as part of the Health System’s Computer Clean Out Program and includes non-refresh and refresh of desktop computers, and the disposal of server and NAS (Network Attached Storage) storage devices.

A. PORTABLE STORAGE DEVICE DISPOSAL PROCEDURE

Users shall dispose of Portable Storage Devices using the following procedure.

1. Health System workforce may call the IS Help Desk to open a ticket for pickup, secure storage, and destruction by the Disposal Vendor.
2. Once the ticket is open, arrangements are made by the IS Help Desk to pick up and transport Device to a secure central holding location maintaining chain of custody.
3. The Disposal Vendor is responsible for pickup and secure transportation of Portable Storage Devices to the vendor’s facilities, maintaining a chain of custody.
4. The Disposal Vendor will destroy Portable Storage Devices in accordance with Department of Defense standards such that they can never be reused.
5. The Disposal Vendor will provide a Certificate of Disposal in compliance with applicable federal, state, and/or local regulations.
6. Certificates of Disposal are maintained by OCIO IT Procurement, and retained for a minimum of six years.
7. For warranty repairs on hardware, users must contact the IS Help Desk to properly destroy the data on storage prior to returning equipment to manufacturer.

B. LEASED EQUIPMENT DISPOSAL PROCEDURE

In accordance with this procedure and *Policy 900.26 Device and Media Control Policy*, any IT Equipment leased to the Health System by a vendor that contains data storage such as internal hard drives (e.g. computers, copy machines, multi-function devices, printers, fax machines, medical equipment, etc.) must be wiped of all data before being returned to the vendor. This includes returns due to service as well as lease-end.

1. Lease agreements will include requirements for the vendor to irretrievably destroy all data on internal storage devices using Department of Defense standards.

2. The vendor will provide a Certificate of Disposal in compliance with applicable federal, state and/or local regulations.
3. Certificates of Disposal are maintained by OCIO IT Procurement and retained for a minimum of six years.

C. COMPUTER CLEAN OUT PROGRAM PROCEDURES

The Health System has contracted with the Disposal Administrator to deploy PCs and peripheral devices throughout the Health System. The Health System has further engaged the Disposal Administrator to fully manage the disposal of equipment replaced during the performance of all of our refresh programs (such as desktop refresh, server refresh, and NAS refresh) in compliance with applicable federal, state and local laws, regulations and standards.

The Disposal Administrator has engaged the Disposal Vendor for disposal services including the vendor managing the complete logistics of the *Computer Clean Out (CCO)* program. As part of the CCO program, when the Disposal Vendor receives the Health System equipment, the Disposal Vendor purchases the equipment and provides the sales price to Disposal Administrator. The Disposal Administrator credits the Health System in the same amount received from the Disposal Vendor minus administrative costs, per Disposal Vendor Contract. The Disposal Vendor then processes the IT equipment for resale or recycling maintaining strict compliance with applicable laws.

The Computer Clean Out program is for the direct removal, sale and proper disposal of computer equipment and Portable Storage Devices from Health System locations. The Disposal Vendor's responsibilities include, but are not limited to:

1. The Disposal Vendor will manage the complete logistics of this program.
2. The disposal of computer equipment and monitors due to obsolescence or damage.
3. The Disposal Vendor recycles and de-manufactures the equipment that no longer has a marketable value.
4. Once the computer equipment is received at the Disposal Vendor Technology Center, the equipment will be sorted and counted.
5. All obsolete or damaged items will be separated, inventoried and prepared for recycling.
6. All Portable Storage Devices will be destroyed in accordance with local, state and federal regulations, providing the Health System with a Certificate of Disposal.
7. Certificates of Disposal are maintained by OCIO IT Procurement, and retained for a minimum of six years.
8. Marketable computer technology will be sorted into categories by machine type.
9. After the inventory is complete, the Disposal Administrator will be provided with a detailed report by the Disposal Vendor.
10. The Disposal Vendor will begin the sale of equipment through various disbursement options. The Disposal Vendor continually enhances its network of distributors both globally and nationally which helps to increase values given to the Health System.
11. While it is the goal of the Disposal Vendor to maximize the return value on the used equipment, the vendor's first priority is to maintain strict compliance with confidential data, recycling and disposal regulations.

Refresh Disposal Procedure

1. The Disposal Administrator uses the Refresh master list to provide work detail to the Disposal Administrator Surveyor.
2. The Disposal Administrator Surveyor creates a change order for the Refresh of the PC or Laptop, which incorporates a work flow task for disposal.
3. The Disposal Administrator Coordinator takes ownership of the change order and assigns the Refresh task to the Disposal Administrator Installer.
4. The refreshed machine is picked up by the Health System or Disposal Administrator van and brought to the Health System's secure central storage facility.
5. The Disposal Administrator enters the data in the asset disposal database.
6. The Disposal Administrator's Hardware coordinator separates hard drive(s) from equipment and assists with tagging, scanning, inventorying and shelving equipment.
7. The Disposal Administrator arranges for secure pick up and transportation by the Disposal Vendor and provides a Refresh pickup report.
8. The Disposal Vendor picks up the Refresh equipment from a central location.
9. All equipment is scanned out of inventory and a sign-off pickup list is obtained by the Disposal Administrator, maintaining chain of custody.
10. The Disposal Administrator closes the change order and updates the asset disposal database.
11. The Disposal Vendor processes the equipment, records assets, installs and wipes hard drives using Department of Defense wiping protocol.
12. The Disposal Vendor provides Certificate of Disposal information and online asset tracking.
13. The Disposal Vendor provides the Certificate of Disposal which notes disposal has been completed in compliance with applicable federal, state and/or local regulations for all equipment received from the Health System.
14. Certificates of Disposal are maintained by OCIO IT Procurement, and retained for a minimum of six years.

Non-refresh Disposal Procedure

1. A Health System change order ticket indicating serial numbers of equipment is provided to the Disposal Administrator.
2. The Disposal Administrator will arrange for secure pick up and transportation of items listed in the ticket from Workforce staff. The Health System or Disposal Administrator van drops off equipment to the Health System's secure central storage facility.
3. The Disposal Administrator enters the data in the asset disposal database.
4. The Disposal Administrator's Hardware Coordinator separates hard drive(s) from equipment and assists with tagging and shelving all Non-Refresh equipment.
5. The Disposal Administrator contacts the Disposal Vendor and provides a Non-Refresh pickup report and schedules the pickup.
6. The Disposal Vendor picks up equipment from a central location. For bulk Non-Refresh location-specific pickups, the Disposal Vendor will pick up from specific locations.
7. The Disposal Vendor will maintain chain of custody by signing off on equipment pickup. A Pickup report will be provided to the Disposal Administrator.
8. The Disposal Administrator closes the change order and updates the asset disposal database.

9. The Disposal Vendor processes the equipment, records assets, installs and wipes hard drives using Department of Defense wiping protocol.
10. The Disposal Vendor updates online asset database tracking.
11. The Disposal Vendor provides the Certificate of Disposal which notes disposal has been completed in compliance with applicable federal, state and/or local regulations for all equipment received from the Health System.
12. Certificates of Disposal are maintained by OCIO IT Procurement, and retained for a minimum of six years.

Marketable Computer Technology

The assets received by the Disposal Vendor are considered marketable computer technology and retain a Fair Market Value. The Disposal Vendor will provide to the Disposal Administrator a sales report about all products sold on a dedicated Web site secured by a logon and password. This equipment will have all data eliminated in accordance with applicable federal, state and local requirements before resale.

Obsolete Equipment

There is no fair market value associated with obsolete equipment. Obsolete equipment will be properly recycled (after all data has been eliminated) in accordance with all federal, state and local requirements.

Equipment Recycling

All non-working and obsolete equipment, terminals and CRTs received by the Disposal Vendor will be recycled. A Certificate of Recycling is provided indemnifying the Health System of any responsibility related to the recycling and disposal of such equipment. The Disposal Vendor's affiliated recycling partner operates in accordance with all federal, state and local regulations.

Security

The Disposal Vendor's warehouse facility will be secured, alarmed and monitored. Access to the warehouse shall be controlled via badge access for entry into the facility. Dock doors shall remain locked and secured during normal operating hours. The Disposal Vendor will allow scheduled inventory audits and inspection of Health System equipment while stored at the Disposal Vendor facility(ies) with 24-hour notice. The Disposal Vendor will provide the Health System with a physical security attestation of controls implemented.

ENFORCEMENT

Users should report any violations of this policy immediately to his or her manager. If appropriate, the violation should be escalated and reported to the IS Help Desk or the Office of Corporate Compliance Help Line. Anyone found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or engagement, as applicable, in consultation with Human Resources.

CONTACT INFORMATION

| What | Where |
|--|--|
| NS-LIJHS Help Desk | (516) (718) (631) 470-7272 |
| NS-LIJHS Help Desk Email | servicedesk@nshs.edu |
| OCIO Security Email | security2@nshs.edu |
| Office of Corporate Compliance | (516) 465-8097 |
| Office of Corporate Compliance Help Line | (800)-894-3226 |
| Office of Corporate Compliance Website | www.northshore-lij.ethicspoint.com |

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- 900.12 Data Classification and Handling Policy
- 900.26 Device and Media Control Policy
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- PCI DSS v2.0 <https://www.pcisecuritystandards.org>

CLINICAL REFERENCES

None

FORMS

None

| APPROVAL | |
|---|----------|
| System P&P Committee | 11/21/13 |
| System PICG/Clinical Operations Committee | 12/12/13 |

Versioning History:

New System Policy

Internal Versioning History

Internal IS Policy since 2006

12/08

9/10