Responsible Disposal of Electronic Assets Policy

Effective Date: June 20, 2022

Purpose

The purpose of this policy is to establish a standard for the responsible management of electronic assets at the end of operational life. This policy noted below does not apply to non-physical assets, such as software licenses.

This policy allows NetScout to ensure the most effective use and management of all electronic assets and responsible recycling of electronic waste.

Definitions

Media: Any Device that may contain or store data

Policy

In accordance with the NetScout Environmental Policy, NetScout is committed to reducing the environmental impacts of company operations and fully complying with all applicable laws and regulations relating to electronic waste.

Coverage

This policy applies to all electronic assets at end of use and operational life, including desktops, laptops, servers, printers, monitors, keyboards, mobile devices, and similar assets.

NetScout departmental managers are encouraged to periodically assess the usage of all electronic assets within their department and decommission any assets which are no longer required.

The policy applies whether the assets are capitalized or not capitalized. Capitalized assets have an “asset tag” affixed to them and are tracked by the NetScout IT organization.

Appropriate Disposal

Whenever possible, NetScout will seek to re-use and re-deploy functional electronic assets.

- If assets cannot be redeployed internally, NetScout will consider if the asset is eligible for donation to a non-profit organization(s) that meet the guidelines of the Heart of Giving program.
    - You must reach out to the Director of Heart of Giving to confirm that the charity interested in receiving the donation is an approved charity under the Heart of Giving Program.
- If an asset cannot be reused, it must be “scrapped” and sent for recycling. Before recycling appropriately, it is critical to complete all data destruction requirements as set out by the IT Security Team. Items marked for scrap are not available for other use.
- In either situation, a ticket that tracks the disposal must be opened and appropriate disposal methods must be followed. Please follow the steps in Appendix A to determine what the appropriate steps are for disposals and donations.

Disposal/ Donation Process

Whenever electronic assets are determined to be no longer required for example, replaced with a newer system during the tech refresh cycle or have reached the end of their operational life, the following process must be followed:

- Open a new IT Ticket, identifying the assets to be disposed of (donation is a special type of disposal) and the reason(s) for that disposal.
- Typical reasons for disposal are:
  - Equipment no longer required
  - Occupying storage space and not needed/obsolete equipment
  - Equipment defective and not economical to repair
- Remove all data from the assets to be disposed of.
- Return the assets to the location as defined and documented in the IT ticket.
- Prior to being disposed of externally, IT shall be responsible for removing those assets from the asset tracking system.
- Appendix A contains detailed steps to determine whether the disposal should be donated or scraped, and the steps to follow for each situation. This process must be followed for every disposal.

Note: NetScout assets must not be sold, loaned, or donated to employees nor the family or friends of employees.

Data Deletion Requirements

IT will ensure the removal of all NetScout data and software from the asset prior to disposal. Data deletion methods must meet NIST 800-88 standards.

- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and physically destroyed. Hard drives must also be removed and rendered unreadable (drilling, crushing or other demolition methods).
  - If physical destruction is not available, a three-pass hard drive wipe is **mandatory** to comply with NIST 800-88 standards. NETSCOUT IT Security recommends using Dell's *Data Wipe* in the Dell BIOS or using Apple's Disk Utility's *secure erase* option.
  - If neither the Dell Data Wipe or Apple Disk Utility are available, the free, open-source utilities DBAN and nwipe are also options (as long as a 3-pass wipe option is used within these programs).
- NETSCOUT recognizes that there are some use cases where USB Flash Drives are required for certain job functions, such as within R&D and Manufacturing. In the event that a flash drive reaches its end of life, they must also abide by the data deletion requirements set forth by this policy.
- Asset numbers and/or stickers must be removed from all assets before disposal.

Vendor Requirements

When the scrapping of electronic assets is the only option, NetScout partners with local vendors that meet the following minimum requirements:

- Responsible Recycling (R2) or e-Stewards certified for recycling of electronics
- Letter of Destruction - Provide reporting to identify assets and weight of materials received for recycling

International Collection Sites

To assist with the disposal process, two international sites have been established **Bangalore** for our Asia Pacific employees and **Dublin** for our European employees.

TAC Equipment Disposal Guidelines

This applies to all technology equipment and media owned, used, or managed by any NETSCOUT associate that may contain or at any time have contained any confidential or sensitive information derived from, through or by any means of the TAC Customer Service Network.

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is environmentally responsible, often required by law, and through our contractual obligations to customers. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Corporate or customer data, which can contain sensitive information. In order to protect our constituent's data, all storage mediums must be destroyed by a certified media destruction company when it has reached the end of its usefulness.

Technology Equipment Disposal

- When technology assets have reached the end of their useful life they must be sent to the local or regional Information Technology office for proper destruction and disposal.
- An authorized NETSCOUT IT associate will ensure that any media that may contain or at any time during its operation may have contained confidential or sensitive data is securely destroyed in compliance with any industry best practices, applicable laws, and regulations. At a minimum, all hard drives must be wiped via an approved NIST 800-88 data sanitization method.
- Any equipment not in working order must be disposed of according to NETSCOUT environmental and corporate guidelines.
- Prior to release from a NETSCOUT premises, all equipment must be removed any NETSCOUT IT inventory systems.

Assistance/ Duty to Report

You are responsible for seeking guidance if you are not sure about the Responsible Disposal of Electronic Assets Policy, and to question or challenge the propriety of situations you suspect may not fully comply with this Policy.

To seek guidance or discuss a concern, you may contact your local manager, local Human Resources business partner, your legal support, or the Compliance Office via MB Compliance@netscout.com. Alternatively, if you do not feel comfortable speaking with someone in person, you may seek assistance online via the secure NetScout Ethics Reporting System ("NSERS") or by calling the number assigned to your location on the NSERS site.

The NSERS is a 24-hour, seven-day-a-week dedicated resource maintained by an independent party to maintain confidentiality and ensure anonymity when requested and allowed by law.

Consequences for Non-Compliance

If you do not comply with this Policy, you may face discipline, up to and including termination of employment.

Related Policies and Resources

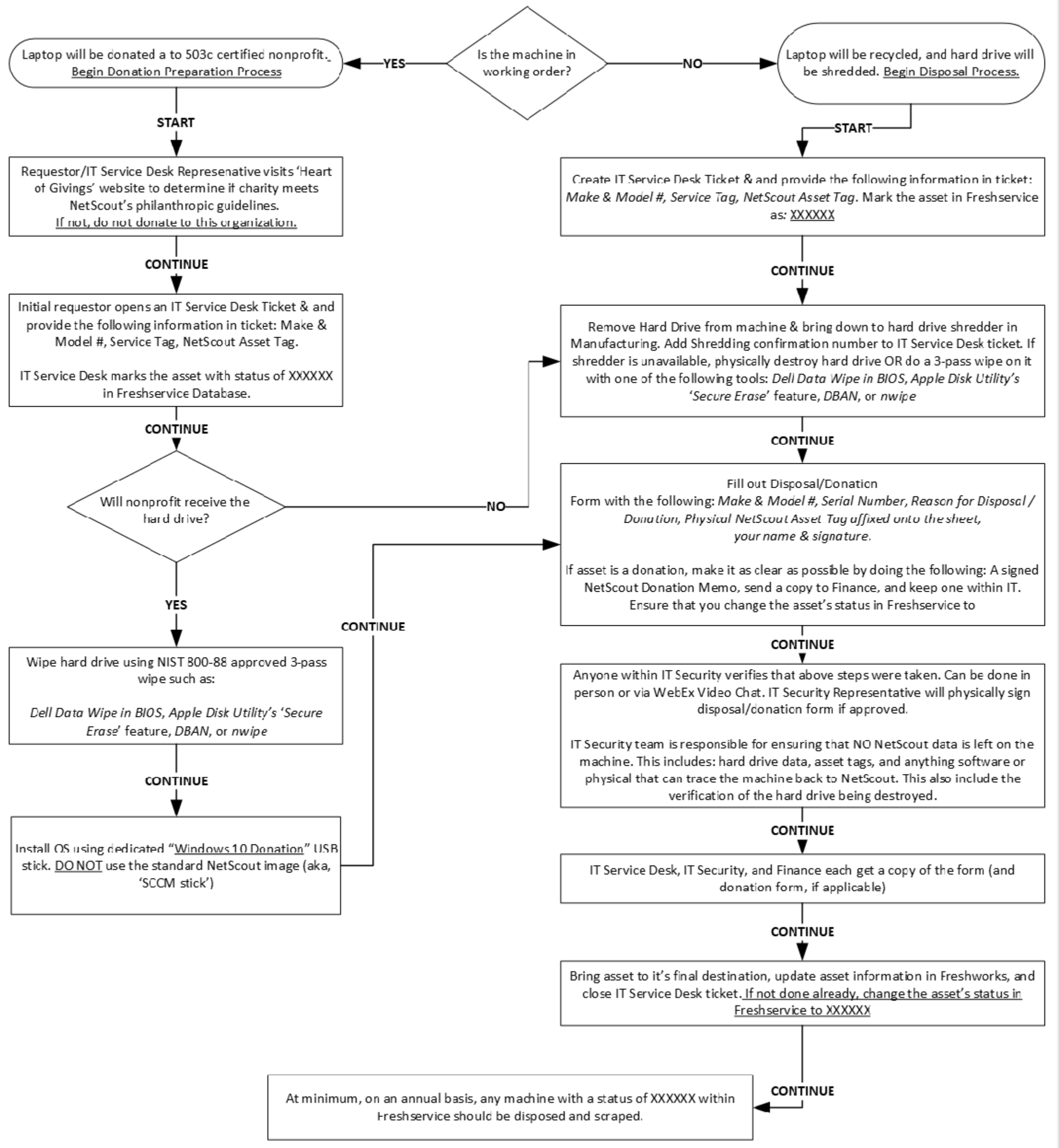
All NETSCOUT Enterprise policies are available on the Scout Policies page here.

Environmental Policy
Procedures for Handling Personal Data

Policy Title:	**Responsible Disposal of Electronic Assets Policy**
Policy Number:	SEC-049
Policy Version:	3.0
Effective Date:	06/2022
Next Review Date:	06/2023
Named Owner:	IT Services
Approved By:	Thor Wallace, CIO
Legal Reviewer:	[if applicable]

Version	**Date**	**Author**	**Comments**
2.0	01 September 2020	Thor Wallace	Updated
2.1	14 April 2021	I. Girolamo	Annual review, minor formatting change
2.2	02 June 2021	I. Girolamo	Included NIST 800-88 three-pass wipe instructions.
2.3	12/14/2021	S. Busby	Updated to include appendix A. Added verbiage to policy referencing the diagram created in appendix A
2.4	15 June 2022	I. Girolamo	Annual review: made updates for clarification, replaced any instance of “should” to “must”, as per AT&T Netbond audit recommendations.
3.0	20 June 2022	S. Busby	Consolidated the TAC Disposal Policy into this one

Appendix A: Disposal Process


Is the machine in working order?
YES
NO
Laptop will be donated a to 503c certified nonprofit. Begin Donation Preparation Process
Laptop will be recycled, and hard drive will be shredded. Begin Disposal Process.
START
START
Requestor/IT Service Desk Represenative visits 'Heart of Givings' website to determine if charity meets NetScout's philanthropic guidelines. If not, do not donate to this organization.
Create IT Service Desk Ticket & and provide the following information in ticket: Make & Model #, Service Tag, NetScout Asset Tag. Mark the asset in Freshservice as: XXXXXX
CONTINUE
CONTINUE
Initial requestor opens an IT Service Desk Ticket & and provide the following information in ticket: Make & Model #, Service Tag, NetScout Asset Tag.
IT Service Desk marks the asset with status of XXXXXX in Freshservice Database.
Remove Hard Drive from machine & bring down to hard drive shredder in Manufacturing. Add Shredding confirmation number to IT Service Desk ticket. If shredder is unavailable, physically destroy hard drive OR do a 3-pass wipe on it with one of the following tools: Dell Data Wipe in BIOS, Apple Disk Utility's 'Secure Erase' feature, DBAN, or nwipe
CONTINUE
CONTINUE
Will nonprofit receive the hard drive?
NO
Fill out Disposal/Donation Form with the following: Make & Model #, Serial Number, Reason for Disposal / Donation, Physical NetScout Asset Tag affixed onto the sheet, your name & signature.
If asset is a donation, make it as clear as possible by doing the following: A signed NetScout Donation Memo, send a copy to Finance, and keep one within IT. Ensure that you change the asset's status in Freshservice to
YES
CONTINUE
CONTINUE
Wipe hard drive using NIST 800-88 approved 3-pass wipe such as:
Dell Data Wipe in BIOS, Apple Disk Utility's 'Secure Erase' feature, DBAN, or nwipe
Anyone within IT Security verifies that above steps were taken. Can be done in person or via WebEx Video Chat. IT Security Representative will physically sign disposal/donation form if approved.
IT Security team is responsible for ensuring that NO NetScout data is left on the machine. This includes: hard drive data, asset tags, and anything software or physical that can trace the machine back to NetScout. This also include the verification of the hard drive being destroyed.
CONTINUE
CONTINUE
Install OS using dedicated "Windows 10 Donation" USB stick. DO NOT use the standard NetScout image (aka, 'SCCM stick')
IT Service Desk, IT Security, and Finance each get a copy of the form (and donation form, if applicable)
CONTINUE
Bring asset to it's final destination, update asset information in Freshworks, and close IT Service Desk ticket. If not done already, change the asset's status in Freshservice to XXXXXX
CONTINUE
At minimum, on an annual basis, any machine with a status of XXXXXX within Freshservice should be disposed and scraped.

NOTE: The disposal form included a line for IT Security team to sign off on the disposal. Anyone working in the IT Security team, can complete and approve the disposal. The IT Security team is responsible for verifying that there is no NETSCOUT data left on the machine. If it is a scrap, the team is also responsible to ensure that the equipment is in the scrap bin