Designated Non-Capital Asset Guidance

Overview

A Designated Non-Capital Asset (DNCA) is defined as any device that stores and processes data with a purchase price under $5,000. In particular, due to the data they contain, DNCAs are a theft risk, and therefore these guidelines are established to address loss prevention and data security. Purchases of any DNCA must follow these guidelines, even if the acquisition cost is minimal.

DNCAs are defined as:

- Desktop computers
- Laptop computers
- Tablets
- Cell phones
- Servers

All DNCAs should be securely stored at all times. This includes physical security of the device as well as the security of the data. All UMD-owned devices should be password protected and utilize full disk encryption. Full disk encryption is currently mandatory for units designated Sensitive for Cybersecurity, it will become mandatory for all units on August 15, 2023.

Roles and Responsibilities

In order to comply with USM policy VIII-1.10 and the USM IT Security Standards, each campus unit is responsible for maintaining appropriate documentation and records about DNCAs. Records include documentation of purchase, receipt, and asset information as outlined below in this document. In addition, procurement policies requiring segregation of duties apply to DNCAs. **The same person cannot be both a Unit Purchaser and an Asset Specialist. These roles must be fulfilled by at least two (2) different people.**

Further explanation of roles and responsibilities related to DNCAs are below.

Role	**Responsibilities**
Unit	College, Division who is responsible for the DNCA.
Unit Purchaser(s)	The individual(s) buying the DNCA. ***The Unit Purchaser(s) cannot be the same person (people) as the Asset Specialist.**

Asset Specialist (Inventory Coordinator)	Individual who is creating and maintaining inventory records. ***The Asset Specialist cannot be the same person as the Unit Purchaser(s).**
Responsible Person (Asset Owner, Custodian)	Person who is responsible for the DNCA or the person that the DNCA is assigned to.
Asset Receiver	Individual who receives (accepts delivery of) the DNCA.

The required separation of duties is the Unit Purchaser and Asset Specialist (Inventory Coordinator). It is possible for the Unit Purchaser or Asset Specialist to also be the responsible person and/or the asset receiver. The Unit Purchaser and Asset Specialist cannot be the same person.

DNCA Purchasing & Receiving

All UMD procurement policies must be followed when purchasing any DNCA. The sensitive nature of DNCAs requires special attention to ensure these assets and records are secure.

All DNCA purchases must:

1. Use the correct object code for DNCAs (see below)
2. Have evidence of receipt

Preferred procurement methods are:

- **Shell Shop**
- **Delegated Purchase Order (PO)**
- **Terrapin Tech**

NOT Preferred procurement method(s) are:

- **Purchasing Card (P-card)** - *DNCAs are **NOT** to be purchased using a P-card*. In rare cases where this is the only purchase option available, the DNCAs must be reallocated to the correct object code (see below).

Object Codes for DNCAs (all items must have a purchase price of less than $5,000)

DNCA Type	***Object Code***
Laptops/desktops	4360
Cell phones	3285
Tablets	3956

Servers	4362

For more information regarding the purchase and receipt of DNCAs please see the DNCA Purchasing & Receiving Job Aid.

DNCA Inventory Management

Designated Non-Capital Asset (DNCA) information must be kept electronically by each unit with appropriate access controls. DNCA inventory records are expected to be accurate and kept up to date.

UMD is in the process of implementing a single central system of record for tracking DNCA inventory. Once that system is deployed, it must be used as the system of record. In the interim, please refer to DNCA Inventory Management Job Aid for guidance on how to properly track DNCAs.

The required data elements that must be kept for DNCAs are noted below. Units may track additional elements to aid in their DNCA maintenance; however, these elements may not be captured in the future university-provided central system for tracking DNCAs.

Required Fields:

- Asset Tag Number
- Asset Tag Type
- Asset Status
- Category
- Make
- Model & Year
- Serial Number
- Encrypted Hard Drive (Y/N)
- Leased (Y/N)
- Research Funded (Y/N)
- Last Inventory Date
- Responsible Person
- Responsible Unit/Department
- Asset Specialist
- Location
- Date in Service (date in use)
- *If Status is Transferred/Re-assigned,*
    - DNCA Transfer Agreement (for inter-departmental transfers only)
    - Sanitization Method Used
    - Date of Sanitization

    - Performer of Sanitization
- *If Status is Retired,*
    - Terrapin Trader Number (for Device shell)
    - Retirement Reason
    - DIT Drop-Off Date
    - Destruction Certificate Date (from DIT)
- *If Status is Lost/Stolen,*
    - UMPD Case Number

For more details on what each field entails and the description of these, please refer to the DNCA Inventory Management Job Aid.

DNCA Asset Tagging

All Designated Non-Capital Assets (DNCAs), including cell phones, must have the appropriate asset tag affixed. This applies to all DNCAs regardless of acquisition method (i.e., leased equipment, government funded, "gifted" DNCAs). All DNCAs should be tagged upon receiving the asset by the Asset Specialist. DNCA tags can be obtained by sending an email to controller@umd.edu.

DNCA Annual Audits

Each unit is expected to perform periodic inventory audits of all Designated Non-Capital Assets (DNCAs), at least once per year, to ensure records are accurate and complete. These audits are to be documented and are subject to review by state and University System of Maryland auditors, as well as UMD's Management Advisory Services.

DNCA Intra-Department (within a department/unit) Transfer

Designated Non-Capital Assets (DNCAs) may be transferred intra-department (between two people within the same department/unit). Prior to the transfer of the DNCA, the units are responsible for wiping the asset using an approved university method. Units must maintain this record of the cleansing for intra-department transfers for three years after the DNCA is retired. After being wiped, the DNCA may be reassigned and the inventory record updated. Please refer to the DNCA Inventory Management Job Aid for guidance on wiping and record keeping expectations.

DNCA Inter-Department (between units/departments) Transfer

Designated Non-Capital Assets (DNCAs) may be transferred inter-department (between departments/units) at the University of Maryland. Units may transfer a DNCA to another unit with vice president or department head approval. This approval/Transfer Agreement must be documented along with the following DNCA information: serial number, category, make, and model & year. This agreement must be documented along with sanitization records. For further

guidance on wiping and record keeping expectations please see the DNCA Inventory Management Job Aid.

DNCA Replacement

DNCAs that are replaced for any reason (leased, damaged, upgraded, warranty, etc.) should be treated as retired. Any new asset acquired to replace the old asset will be treated as a brand new asset with a new asset record and new asset tag.

All records and documentation pertaining to a replaced DNCA (leased, damaged, upgraded, warranty, etc.) shall be retained and kept for a period of at least 3 years.

For more information regarding the inventory management of DNCAs, please see the DNCA Inventory Management Job Aid.

DNCA Retirement

USM IT Security Standards, the UMD policy on retirement of assets, and software licensing terms must be followed when retiring any DNCA. The sensitive nature of DNCAs requires additional steps to ensure these assets and their data are secure.

Data Destruction Guidance

When a DNCA has been identified as needing to be retired, please follow guidance below:

- For DNCAs with removable hard drives, the hard drive should go through DIT's Storage Device Destruction process, and the shell should be sent to Terrapin Trader.
- For DNCAs with non removable hard drives (including cell phones and tablets), please wipe the device and send it to Terrapin Trader.

Records of destruction must be kept for three years after the DNCA has been retired.

Retiring DNCAs Under Litigation Hold

If there are questions as to whether your unit is involved in a litigation hold, please contact DIT's Security Operations Center (soc@umd.edu) before retiring and/or sanitizing any DNCAs.

Retiring Leased DNCAs

For a leased DNCA, the units/departments are required to follow the asset retirement procedures included in the contract. Vendors should provide a certification of destruction to units, and the certificate should be retained for three years after the DNCA has been retired for audit purposes.

Retiring Research/Government-Funded DNCAs

For research-funded DNCAs, the Principal Investigators are required to follow the retirement

procedures, including data destruction, indicated in the grant, contract, or cooperative agreement. Retirement of surplus property originally procured with federal grant or contract funds shall be in accordance with the terms of the grant or contract. Research-funded DNCAs are not to be declared surplus without the express written consent of the owning entity and the approval of the Sponsored Programs Accounting and Compliance (SPAC). Vendors should provide a certification of destruction to units, and these certificates should be retained for audit purposes. If you have any questions about how to handle research-funded DNCAs or want to request an exception, please contact dncacompliance@umd.edu.

Donating DNCAs

Only DNCAs with removable hard drives may be donated. DNCAs with removable hard drives that are for donation must be sent to Terrapin Trader. Before sending DNCAs with removable hard drives to Terrapin Trader, units/departments should ensure all software (including operating systems) and data is securely removed by pulling the hard drive. No DNCA is to leave UMD with UMD data. Units are not authorized to donate devices directly to outside organizations. If a unit/department wishes to donate a DNCA to a particular not-for-profit, school, or government agency, please email dncacompliance@umd.edu for guidance.

Employee Purchase of DNCAs

Units may not give DNCAs away or directly sell them to current or separating employees. DNCAs must be returned by separating faculty and staff. For inquiries on exceptions to this please contact dncacompliance@umd.edu.

Stolen or Lost DNCAs

The responsible person should always keep their DNCA in a secure location. In the event your DNCA is stolen or lost, the responsible person should immediately notify UMPD. In the event the DNCA was stolen/lost outside the state of Maryland, the theft should be reported to the local police department in addition to UMPD. Units must keep a copy of the police report with the DNCA record and update the record to reflect that the DNCA has been stolen.

Once UMPD has been notified of the stolen/lost DNCA, contact the DIT Security Operations Center (soc@umd.edu) and your unit's IT administrator. Depending on your DNCA settings, the DNCA may be locatable, disabled, etc. Update the DNCA status in the inventory records accordingly, and keep record of your correspondence with DIT.

Please note UMD's insurance does not cover replacement costs for stolen or lost DNCAs. Units are responsible for replacing their own missing, stolen, or lost DNCAs.

Payment Card Devices

Payment card devices are considered DNCAs. However, given their unique requirements, they are currently governed by a separate set of UMD procedures. If you have any questions specific to payment card devices please contact pcicompliance@umd.edu.

Exceptions

Any requests for exceptions to these procedures should be sent to dncacompliance@umd.edu.

Violation of Policy/Procedures

Any violations of any UMD policy are subject to disciplinary actions up to and including termination. The university may seek restitution. Criminal charges will be enforced as applicable.

Questions

Contact dncacompliance@umd.edu with questions.