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/Smartphones
- 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 December 31, 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**

Questions:Use ServiceNow

	(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)**
- P-cards **can be used for cell** phones purchased on an official University of Maryland account. Please see cell phone job aid for more information.

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). Best practices include adding a note to your p-card log indicating why a p-card was the best option.

Questions:Use ServiceNow

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 via ServiceNow by each unit. DNCA inventory records are expected to be accurate and kept up to date.

ServiceNow is the single central system of record for tracking DNCA inventory. This platform will enable a standard, uniform asset management process for DNCAs to facilitate compliance for the UMD campus. Use of ServiceNow to record DNCAs is required.

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 sanitizing/wiping the asset using an approved university method. Units must maintain record of the sanitization/wiping for intra-department transfers for three years after the

Questions:Use ServiceNow

DNCA is retired. After being sanitized/wiped, the DNCA may be reassigned and the inventory record updated. Please refer to the DNCA Inventory Management Job Aid for guidance on sanitization/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. Please refer to the DNCA Inventory Management Job Aid for guidance on sanitization/wiping and record keeping expectations.

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

Terrapin Trader is the department responsible for surplus property for the entire campus. Follow this knowledge article to retire a DNCA through ServiceNow with Terrapin Trader.

Data Destruction Guidance
When a DNCA has been identified as needing to be retired, please follow guidance below and work closely with your Asset Specialist:

- Scenario 1
    - DNCAs with HIPAA data
    - DNCAs with CUI data
    - DNCAs that are tied to a litigation hold

Questions:Use ServiceNow

Action – Reach out to IT-Compliance@umd.edu to confirm UMD is in compliance with any regulations tied to destruction of this data.

- Scenario 2
  - DNCA's with removable hard drives

  Action – Use the Terrapin Trader Surplus process and reach out to IT-Compliance@umd.edu if you believe HIGH or RESTRICTED data is being stored on device.

- Scenario 3
  - DNCA's with non-removable hard drives

  Action – Use the Terrapin Trader Surplus process.

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

It is incumbent on the Principal Investigators and support staff to ensure retirement procedures, including data destruction, indicated in the grant, contract, or cooperative agreement are followed. Any questions about your research language should be directed to Sponsored Programs Accounting and Compliance (SPAC)

In most instances, DNCAs purchased with sponsored funding are the property of the University and must follow the same retirement procedures.

In the rare circumstance that your DNCAs are expected to be returned to the sponsor, you can use Object Code 4361 to separately account for these assets. If you have any questions about how to handle research-funded DNCAs or want to request an exception, please contact the DNCA team through ServiceNow.

Questions:Use ServiceNow

Donating DNCAs

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 use the DNCA Exception Request Form.

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. To request an exception please use the DNCA Exception Request Form.

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

To request a DNCA exception to these guidelines click here to access and populate the required "DNCA Exception Request Form" to start the DNCA exception process.

Any questions about the exception process should be submitted through ServiceNow.

Questions:Use ServiceNow

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:Use ServiceNow