1T Dallas County
Office of Information Technology

Customer Centered. Powered by Intellect. Driven by Values.

Dallas County Information Technology
Asset Management Policy

1. Scope

The Dallas County Asset Management Policy applies to all Users (County employees, elected officials, contractors, subcontractors, part-time and temporary workers, individuals telecommuting, and those who have been granted access to County's electronic and computing devices).

Computing resources include all Dallas County-owned, licensed, or managed hardware and software, data, information, information assets, Dallas County-assigned user accounts, and use of the Dallas County network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Because Dallas County owns the network, this Policy applies to technology administered in all departments and divisions, all computers and devices connected (wired and wireless) to the Dallas County network, and to off-site computers that connect remotely to the Dallas County network services.

This policy supersedes all other policies on this topic either written or verbal.

2. Purpose

This document defines the policy necessary to ensure that Dallas County's assets are known, identified, and managed with appropriate protection in place.

3. Policy

Overview

(a) The Dallas County Office of Information Technology is responsible for the management of technology assets and lifecycle processes, including standards, acquisition, management, surplus and long-term planning.

(b) Technology assets are assigned to a specific individuals or locations but remain property of Dallas County.

(c) Technology assets will be utilized until "End of Life" has been reached or as long as it remains practicable and compliant with all Dallas County security requirements.

(d) All technology assets, whether software or hardware, installed must be Dallas County-owned and approved by IT Operations.

(e) All Dallas County assets including both hardware and software must be approved by the IT Security Team.

Asset Types

This Asset Management Policy applies to all devices and accompanying media that fit the following classifications:

- Workstations – desktops or laptops
- Thin-client workstations
- Printers, copiers, fax machines, and multifunction print devices
- Scanners
- Servers

- Network Appliances (e.g., firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
- Private Branch Exchange (PBX) and Voice-over Internet Protocol (VOIP_ Telephony Systems and components
- Internet Protocol (IP) Enabled Video and Security Devices
- Memory Devices
- Monitoring devices
- Televisions
- Mobile devices (e.g., tablet computers, wearable technology, cellular phones, smart phones including BYOD, Microsoft Surface Book, MiFi, tablets, wireless data cards, microcell routers, any mobile device capable of storing County data and connecting to a network (including Wi-Fi connection)(this does not include the pagers utilized by Facilities)

Inventory of Assets

For Existing Assets: The Office of Information Technology shall maintain an inventory of all hardware and software assets in a Content Management Database (CMDB). For initial implementation of this Policy the newly contracted Desktop Support Vendor shall conduct a complete inventory of all current assets upon approval of this Policy. Thereafter, an annual inventory shall be conducted of all existing assets by the Office of Information Technology beginning on October 1st of each year by providing a list of known existing assets to each User department and requiring the User department to verify the list of assets.
For New Assets: Before any new asset is put into service, the asset must first be entered in the CMDB.

The Office of Information Technology shall enact operational controls to enforce this aspect of the Policy for both existing and new assets.

For each asset, at a minimum, the following shall be recorded by the IT Asset Manager:

- Asset type
- Asset brand
- Asset model
- Asset serial number
- Vendor Asset Tag number
- Asset Location (person or physical location)
- Asset owner (biographical and business unit information)
- User assignment of the asset
- The classification of the asset
- Trackability and method of tracking of the asset
- Acquisition Date and method of acquisition of the Asset
- Obsolescence Date of the Asset
- Automated Scan method
- Last Automated Scan Date
- Warranty type and term of the warranty

Inventory of Software Assets

(a) Software licenses will be assigned to a user or a specific machine, dependent upon software type or business use.

(b) Installation of business-related, no cost software (e.g. – Adobe Acrobat Reader) must be evaluated and approved by the Office of Information Technology.
(c) Augmentation to any software, application or operating system security configuration by a user is prohibited. All security configurations must be approved by the IT Security Team.
(d) Non-Dallas County owned User supplied software is strictly prohibited.
(e) Duplication of licensed software is a violation of copyright laws and strictly prohibited.
(f) For software assets, at a minimum the following shall be recorded in the CMDB by the IT Asset Manager, in addition to the minimum requirements above:
    (1) Software Name
    (2) Software Version
    (3) Software License Key
    (4) Software License Expiration
    (5) Software License Entitlements
    (6) Software License Type
    (7) Name of Machine it is Installed on
    (8) Name of Individual Software is Assigned to
    (9) Date Acquired
    (10)Upgrade version
    (11)Renewal details – amount and frequency

Asset Moving or Transferring

When an asset is being moved from one location to another, it must be updated in the CMDB with the new information. This may include moving a computer asset to a new employee that will be responsible for the asset, moving a copy machine or printer to a new office, or transferring a software license. It is the responsibility of the User department to promptly contact the IT Asset Manager in the Office of Information Technology when an asset has moved, so that the CMDB can be updated. The Office of Information Technology shall enact operational controls to enforce this aspect of the Policy.

Asset Maintenance

All device maintenance issues, and requests for servicing, repairing, or replacing equipment shall be performed by the IT Asset Manager.

Asset Surplus

When equipment is no longer useful or needed, a P280 property transfer request can be approved for assets to be transferred to a secure “surplus location” currently designated by the Office of Information Technology if the asset is in working order. The person or department responsible for the equipment must inform Dallas County’s Fixed Asset Division of the Purchasing Department about the equipment no Longer needed. The Fixed Asset Division will review, track, and issue an approved work order number to the IT Asset Management team. This equipment will then be collected, and the asset information will be updated in the asset tracking database to show the correct “surplus location.”

Selling, Lease Return, or Decommissioning

Technology assets that have reached End of Life or are considered surplus must be updated in the CMDB with correct and up-to-date information including, but not limited to:

- Entity that purchased or claimed the asset
- Reason for sale or decommission

- Date of sale or decommission
- All devices reaching end-of-service must undergo the process outlined in the Data Disposal and Sanitation Policy. The IT Asset Manager must be updated prior to transferring ownership of a device to comply with this Policy so that the CMDB can be properly updated.

Lost or Stolen Assets

Prompt and appropriate action will be taken to locate and recover lost or stolen technology assets. Department heads and Elected officials shall follow the procedure detailed in Dallas County Code Section 90-471 for lost or stolen assets. Upon receiving notice of a lost or stolen item, the County Auditor and Purchasing Agent shall notify the IT Asset Manager and the Service Desk of the loss or theft. Lost or stolen assets must be both frozen, deactivated, or wiped as determined by the IT Security Team to protect the County's confidential data. The CMDB shall be with corrected with up-to-date information including, but not limited to:

- Asset location set accordingly to "Lost or Stolen"
- Notation of person responsible for asset
- Sheriff's Department report number
- Date of loss or theft
- Notation of replacement equipment (if applicable)

Termination of Access and Return of Assets

All employees and external party users must return all Dallas County assets in their possession upon termination of their employment, contract, or agreement. Upon notice by and individual or entity of its immediate or pending termination of their relationship with Dallas County the procedure in Dallas County Code Section 74-836 et seq., shall be followed.

4. Periodic Reviews

This Policy will be reviewed and updated on an annual basis by the Office of Information Technology and the Chief Privacy Officer.

5. Enforcement and Exception Handling

All the Users must follow this Policy. Failure to comply with the Criminal Justice Information Policy (CJIS), Dallas County Code, other applicable data privacy regulations, and Dallas County Security Policies can result in a loss of access and/or disciplinary actions, up to and including termination of employment, contracts and/or other relationships. Additionally legal action may also be taken in response to violations of applicable regulations and laws.

Requests for exceptions to this Policy should be submitted to the ServiceDesk and routed to the Security Team. Exceptions will be permitted only upon receipt of written approval from both the Dallas County Chief Information Officer and Chief Privacy Officer.

7. Revision History

Date:	***version #:***	***Description:***	***Updated by:***
06/02/2023	1.0	Initial Draft	Kroll
7/6/23	1.1	Revised Draft	Randall Miller, CPO
7/18/23	1.2	Revised Draft	Randall Miller, CPO