Document Code No.: ITG-P-21-04
Title: King County Asset Management Policy
Affected Agencies: Countywide
Authorities: King County Code KCC 2A.380
Keywords: Technology Asset Management
Sponsoring Agency: Department of Information Technology

Chief Information Officer Signature: DocuSigned by: 920AF9FCB611460...
Date signed and effective: 2/16/2021

I. Purpose:

The purpose of this policy is to establish the requirements for the inventory of King County's technology assets. This includes hardware, software, data and certain identities (such as default identities created by technology manufacturers or special purpose identities like King County social media accounts). This policy reflects King County's pro equity and social justice commitment. Implementation of this information security policy aligns and complies, in every regard, with King County's equity and social justice policies and practices.

II. Applicability and Audience

A. Users

This policy applies to all workforce members responsible for technology asset ownership and support as well as any workforce members involved in purchasing, procuring, creating, or developing technology assets on behalf of King County.

B. Technology Assets

This policy applies to all technology assets used to support King County operations and service delivery that can create, process, transmit or receive, and/or store data or are capable of connecting to a network. Personally owned computers, tablets, mobile phones and personal home office equipment are not in scope of this policy.

Examples of assets in scope include:

1. Computers, laptops, tablets, VoIP phones, mobile phones
2. Printers, copiers, scanners, and fax machines
3. Network, server, and telecommunications infrastructure
4. Small portable storage devices (e.g., USB "thumb drive," USB "jump drive," USB "storage stick," USB "flash drive," etc.) that will be used to store regulated, sensitive or confidential information (category 3 or 4 data as defined in the Information Classification Policy)
5. Industrial Control Systems (ICS)
6. Supervisory Control and Data Acquisition (SCADA) systems
7. Internet of Things (IoT) devices or specialized technology devices including audio/visual equipment, medical equipment, camera systems, payment card terminals, vehicle management systems, Unmanned Aerial Vehicles (UAV), facility

lighting systems, Heating, Venting, and Air Conditioning (HVAC) systems and other less common devices that have the ability to connect to and communicate over a network or interact with data

8. Commercial off the shelf (COTS) or custom developed software applications deployed within King County's owned and operated environments or deployed from a cloud or hosted provider environment
9. Software components that can be configured with a distinct network address and/or has the ability to store data (e.g., logic apps, functions, application programming interfaces (API), other software service endpoint technology)
10. Structured data such as a database as well as unstructured data collections, groups, or file shares (not individual files)
11. Account credentials used to communicate to the public through technology like social media on behalf of King County or credentials for third-party systems and services used for the purposes of King County operations or service delivery
12. Technology assets that support King County operations and service delivery but are not directly owned by King County (e.g., internet service provider equipment located within King County facilities, equipment provided by the State of Washington, partner or third-party equipment located in King County facilities or connected to King County owned and operated networks, etc.).

C. Exceptions

Requests for exceptions to this policy must follow the Department of Information Technology (KCIT) information security policy exceptions handling process. Please open a ticket with the helpdesk to request a policy exception.

III. Definitions

All definitions are contained within the King County Information Security Policy and Standards Glossary.

IV. Policy

A. Inventory Systems of Record

The Department of Information Technology (KCIT) is responsible for providing countywide systems of record as defined in the Asset Management Standard. Workforce members authorized to purchase, procure, create or develop technology assets on behalf of King County are required to ensure that all King County technology assets have at least the minimum required information in this policy entered into the central systems of record where the value exists (not all values in the minimum information set may exist for every possible asset). Departments and agencies who maintain separate systems of record for technology assets are required to ensure that the minimum required information for each technology asset is synchronized to the central systems of record on at least a daily basis.

B. Hardware Asset Inventory

A hardware asset inventory consists of key data elements for tracking hardware assets through their lifecycle. Hardware assets shall be inventoried in the approved system of record as identified in the Asset Management Standard. The following data values are required to be reviewed and entered if the value exists for hardware assets:

1. Asset Owner (e.g., department that purchased the asset);
2. Technology Support Owner (e.g., Department of Information Technology (KCIT), Vendor Name, Department, Agency);
3. Employees authorized to approve access to the Asset
4. Asset Make and Model;
5. Asset Manufacturer Serial Number;
6. King County Asset Tag;
7. Employee, Team or Group, or Division the Asset is issued to;
8. Asset Type (e.g., physical, virtual);
9. Asset Class (e.g., laptop, server, software, network switch, firewall, etc.);
10. Asset Location (e.g., Chinook Building, Employee Issue, etc.);
11. Information Classification (refer to the Information Classification Policy);
12. Impact (refer to the Information Classification Policy);
13. Essential Service Status (e.g., is, is not);
14. Asset Value at Purchase;
15. Expected Asset Lifecycle Duration;
16. Asset State (e.g., active, deprecated, decommissioned, unknown); and
17. Asset Service Dates (i.e., purchased, issued, decommissioned, surplus, etc.).

C. Software Asset Inventory

A software asset inventory consists of key data elements for tracking software assets through their lifecycle. Software assets shall be inventoried in the approved system of record as identified in the Asset Management Standard. The following data values are required to be reviewed and entered if the value exists for software assets:

1. Application Owner (Default is Department or Agency Director or Presiding Judge);
2. Technology Support Owner (e.g., Department of Information Technology (KCIT), Vendor Name, Department, Agency);
3. Employees authorized to approve access to the Asset
4. Application Name;

5. Application Unique ID (e.g., auto or manually assigned, a portfolio management system ID, etc.);
6. Application Type (e.g., COTS, third party custom, open source, custom);
7. Application Scope (e.g., team, division, department, enterprise, public, external partners, etc.);
8. Technology Support Contact Information (e.g., website or contact where support or can be accessed)
9. Information Classification (refer to the Information Classification Policy);
10. Impact (refer to the Information Classification Policy);
11. Essential Service Status (e.g., is, is not);
12. Application State (e.g., active, deprecated, decommissioned, unknown); and
13. Application Service Dates (e.g., purchased/developed, initial go live date, last major revision).

D. Data Asset Inventory

A data asset inventory consists of key data elements for tracking both structured and unstructured data not at the individual record level but at a level such as a database, network share, document library, or other logical grouping that represents the primary purpose or general use of the data. Data assets shall be inventoried in the approved system of record as identified in the Asset Management Standard. Records management and retention requirements are not in scope of this policy (please refer to the King County Records Management Program or Department or Agency Records Officers). The following elements are required to be reviewed and entered if a value exists for data assets:

1. Data Owner (Default is Department or Agency Director or Presiding Judge);
2. Data Custodian (Default is Technology Support Owner)
3. Employees authorized to approve access to the Asset
4. Data Elements if Structured (e.g., Name, Date, Address, etc.);
5. Data Purpose (e.g., Transit Routes, Team File Share, Private User File Storage)
6. Information Classification (refer to the Information Classification Policy);
7. Impact (refer to the Information Classification Policy);
8. Data Storage Type (e.g., MS SQL, Azure SQL, OneDrive, SharePoint, CIFS, File Server, etc.);
9. Data Storage Location(s) (e.g., File Server Name, Database Server Cluster/Instance Name, REST endpoint, etc.);
10. State of the Data Asset (e.g., active, decommissioned, unknown); and

11. Data Asset Service Dates (e.g., created, destroyed, dispositioned, etc.).

E. Identity Asset Inventory

Certain identities are created on behalf of a specific workforce member so they may access County technology resources. For example, most King County workforce members are issued a username and a password that is used to log into workstations, access email, and for group memberships that provide access to certain technology resources or email distribution lists. These identities are not the types of identity assets covered by this policy and instead are covered by the Access Management Policy and Identification and Authentication Policy.

In contrast, identities that are created on behalf of King County or its departments, agencies, or lines of business with external service providers, machine and service accounts, manufacturer provided and local system accounts, and social media accounts are considered identity assets covered by this policy.

Identity assets shall be inventoried in the approved system of record as identified in the Access Control and Authentication Management Standard. Identity assets with credentials (e.g., usernames and passwords) must only be stored in the approved system of record for identities which must include security controls for protecting credentials (i.e., may not be stored separately in a spreadsheet in plain text). The system of record for identities must also include the ability to restrict access to individual records using role based access control.

The following elements are required to be reviewed and entered if a value exists for identity assets:

1. Identity Owner;
2. Username;
3. Password;
4. Uniform Resource Locator (URL) if web-based system;
5. System Identification (e.g., Server Name, Social Media Platform, King County Asset Tag ID, Portfolio Management System ID, or other system identifier for which the identity is used);
6. Description of Purpose;
7. Documentation of relevant associated information (e.g., password reset questions, if a multifactor authentication token is used, etc.);
8. Information Classification of System the Identity is used to access (refer to the Information Classification Policy);
9. Asset Service Dates (e.g., created, modified, decommissioned, etc.); and
10. Asset State (e.g., active, deprecated, decommissioned, unknown).

F. Audit and Physical Inventory

The Department of Information Technology (KCIT) will conduct audits of asset inventories on a periodic basis and the degree of variance from the system(s) of record must be corrected by the owner of the asset. If significant variations are identified, a root cause analysis will be performed, and process changes must be implemented to address the root cause of significant variance. A full inventory of physical hardware assets will be performed by asset owners and the Department of Information Technology (KCIT) at least once every two years.

G. Ownership of Assets

All King County technology assets must have a designated Technology Asset Owner and a Technology Support Owner which includes both a department or agency level owner and the accountable individual role. Technology Asset Owners are by default the Department or Agency Director or Presiding Judge of the department or agency where the asset was created or purchased and are responsible for ensuring compliance with King County information security policies and standards. The Chief Information Officer is by default the asset owner for enterprise countywide identity, unified communications, cloud, server, and network infrastructure. Asset Ownership may be delegated. The Department of Information Technology (KCIT) is responsible for providing technical guidance and implementation support to Technology Asset Owners and Technology Support Owners to achieve compliance with information security policies and standards.

H. Acceptable Use of Assets

The acceptable use of assets is governed through the Acceptable Use Policy. The Technology Asset Owner must ensure that all users of the asset are made aware of the information security requirements as well as their responsibility to return hardware assets issued directly to them upon termination.

V. Implementation Plan

This policy becomes effective for countywide use on the date that it is signed by Chief Information Officer. All new technology implementations and new material changes to existing technology implementations must ensure compliance with this policy as of the effective date. All other technology implementations must be brought into compliance within four years after the effective date.

VI. Maintenance

A. This policy will be maintained by the Department of Information Technology (KCIT), Office of the CIO, or its successor agency. This includes, but may not be limited to:

1. Interpretation of this policy
2. Ensuring this policy content is kept current
3. Recommending updates to this policy and related resources

4. Developing an escalation and mitigation process if an Organization is not in compliance
5. Assisting Organizations to understand how to comply with this policy
6. Monitoring annual compliance by Organizations

B. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the Office of the CIO, or its successor agency prior to the expiration date.

VII. Consequences for Noncompliance

Violations of this policy may be grounds for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges.

VIII. Appendix A: References

- Information Classification Policy
- Acceptable Use Policy
- Access Management Policy
- Identification and Authentication Policy
- Information Security Policy and Standards Glossary

IX. Appendix B: Relevant Compliance Requirements

This section provides references to relevant regulations and standards that apply to King County. This section does not replace the authoritative source and is just a reference to assist with further research. Please use the Compliance Standard and Section No. to further research the entirety of the regulation, framework or standard from the authoritative source.

Compliance Standard	Section No.	Description
HIPAA	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	164.306(b)	Flexibility of Approach
	164.310(d)(1)	Device and Media Controls
CJIS Policy v5.9	5.4	Auditing and Accountability
	5.13.1	Wireless Communications Technologies
	5.13.4	System Integrity
PCI DSS v3.2.1	2.4	Maintain an inventory of system components that are in scope for PCI DSS.

	9.9.1	Maintain an up-to-date list of devices. The list should include the following: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification.
	11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.
	12.3.3	A list of all such (critical technology) devices and personnel with access.
	12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).
NIST CSF	ID.AM	Asset Management
NIST 800-53r5	CM-8	System Component Inventory
	PM-5	System Inventory
	CP-2 (8)	Contingency Plan: Identify Critical Assets
CIS Controls v7.1	1.4	Maintain Detailed Asset Inventory
	2.1	Maintain Inventory of Authorized Software
	4.1	Maintain Inventory of Administrative Accounts
	13.1	Maintain an Inventory of Sensitive Information