| Information Security and Technology Policy | Number 6.0 | | Policy Owner |
|---|---|---|---|
| | **Data and Asset Classification** | | Civic Innovation & Technology |
| | Effective | **01/01/2017** | |
| | Last Revision | **12/07/2021** | |

# 6. Data and Asset Classification

A risk-based information data and computer asset classification scheme shall be established in order to ensure that data is handled and managed appropriately. Data and computer assets shall be classified in a manner that indicates the need, priorities, and expected degree of protection appropriate to the nature of the data and the potential impact of misuse.

This policy reviews the following areas:

## 6.1 Responsibility for Computer and Information Assets

All computer and information assets ("data assets") shall be accounted for and have an assigned owner. Acceptable use of Metro data assets shall be understood by all employees and contingent staff.

### 6.1.1 Ownership of Computer Assets and Data

Unless specifically identified and approved in writing by the County Attorney's Office, all information possessed or used by a particular department and all information stored and processed over the Metro's technology and information systems are the property of the Metro and shall have a designated Data Owner. Metro employees and contingent staff have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state and local laws of the United States and, where applicable, foreign laws.

a. All physical computing assets shall have an assigned Asset Owner.

b. All production information possessed or used by a department or organization within Metro shall have a designated Data Owner. Ownership and custodianship of assets shall be documented.

HIPAA: 164.310(d)(1)(iii), ISO: 7.1.2

### 6.1.2 Data Governance

The accountability and responsibility for ensuring the confidentiality, integrity and availability of Metro owned and managed data shall be defined.

a. The below matrix provides definitions of the three defined data roles. DoIT is responsible for developing the roles and responsibilities for proper data handling procedures.

| | |
|---|---|
| *Data Owner* | The individual(s), normally a manager or director, who has accountability and responsibility for the integrity, accurate reporting and use of computerized data. This individual(s) typically exist within the department that generated the data and is ultimately accountable for its accuracy and proper handling. |
| *Data Custodian* | The individual(s) and department(s) responsible for the storage, safeguarding and availability of computerized data. DoIT is a primary Custodian within Metro. |
| *Data Consumer* | The individual(s) and department(s) that use provided data to perform a job responsibility including the possible generation of new data. A data consumer may also be a data custodian if that person transfers data from its original location.<br>Example: If an employee or contingent worker transfers data from a server or website to their workstation, that individual is not only a consumer but also a custodian of that data and is responsible for its proper handling. |

### 6.1.3 Acceptable Use of Computer Assets

The acceptable use of resources, information and assets shall be documented and understood by all staff (see *Acceptable Use and Personnel Security Policy*). Use of these resources is intended for business purposes in accordance with individual job function and responsibilities. Personal use which is limited and in accordance with Metro's Ethics Ordinance, Personnel Rules and other Applicable Use policies is permitted. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the Metro, consumes excessive time, or violates departmental policy. The privilege of limited personal use may be revoked or limited at any time by Metro or Department officials.

a. The Cybersecurity Office is responsible for defining acceptable use of resources, information and assets including appropriate labeling and handling procedures. In the absence of specific guidance, Data Owners and Department Management are primarily responsible to develop recommendations and minimum standards. HIPAA: 164.310(d)(1)(iii), ISO: 7.1.3, PCI: 12.3, 12.3.5

b. An up-to-date list of all technologies as approved/coordinated by Operations and Enterprise Architecture shall be maintained and readily available. PCI: 12.3.7

### 6.1.4 Inventory of Computer Assets

An inventory of all information assets, including systems, software, and service providers, shall be kept current at all times.

a. Operations and Enterprise Architecture shall compile and maintain a data repository catalog on all third party software-related assets (e.g., application software, development tools and all third party purchased software). This catalog shall be reviewed and updated annually. The catalog should contain descriptive asset information (e.g., vendor, logical locations/associated applications or systems, physical location (if applicable), owner/responsible party, information custodial responsibilities, information classification and criticality level). Business Relationship Managers are required to assist in maintaining this catalog and should communicate any changes or additions.
HIPAA: 164.310(d)(1)(iii) ISO: 7.1.1

b. Operations and Enterprise Architecture shall compile and maintain a data repository catalog of all physical assets owned by the Metro. This catalog shall be reviewed and updated annually. The catalog shall contain descriptive asset information. Business unit managers are required to assist Operations and Enterprise Architecture in maintaining this catalog and should communicate any changes or additions in a timely manner.
HIPAA: 164.310(d)(1)(iii), ISO: 7.1.1, PCI 12.3.3

c. Return of Assets - All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. ISO 27001(A8.1.4)

## 6.2 Information and Data Classification

Information classification is based on the level of sensitivity of the data and the potential impact of inappropriate handling should the confidentiality, integrity or availability of the information or data compromised. A classification scheme, which establishes the baseline security controls for safeguarding information, shall be used to ensure appropriate security protections are placed around information during handling.

### 6.2.1 Information and Data Classification Guidelines

An information classification scheme shall be used throughout the organization to protect Metro's assets.

a. The Cybersecurity Office is responsible for defining the Information Data Classification scheme.

b. Technology Operations and Enterprise Architecture is responsible for management oversight of all information assets and shall define procedures for proper data identification and handling. HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

c. Data Owners or an assigned Data Custodian is responsible for defining the classification of an information asset. ISO: 7.2.1

d. It is the Data Owner or delegated Data Custodian's responsibility to monitor information assets and continuously review the information's classification. The Data Owner or delegated Data Custodian shall sponsor a formal declassification effort before information can be downgraded to a lower classification, based upon the definitions of the classification.
ISO: 7.2.1

e. Employees, contractors, and vendors shall protect all Metro information in any format (e.g., hard copy, disk, tape, flash drive, etc.) at the level commensurate with its value as determined by its information classification. These standards mitigate the risk that information of different classification levels be inadvertently combined and released. Correctly classified information with proper controls can be instituted to manage the dissemination of information throughout the Metro environment.
HIPAA: 164.310(d)(1), ISO: 7.2.1

### 6.2.2 Information and Data Classification Scheme

Metro has a four-tier classification system consisting of “Public,” “Internal”, “Sensitive” and “Confidential” levels of classification.

**a.** **Public** Information is defined as information that is intended for unrestricted public disclosure and is not exempt from disclosure under the Kentucky Open Records Act (KRS 61.870 to KRS 61.884) (KORA).

*Examples include open datasets, announcements, employment advertisements, press releases and marketing materials.*

**b.** **Internal** Information is defined as information that is related to the day to day operations of Metro departments and services. All internal data is subject to the Kentucky Open Records Act and if disclosed would have minimal to no impact on the confidentiality, integrity or availability of Metro data or computer assets. Internal information can be exempt from disclosure under KRS 61.878 or other laws, and the advice of the County Attorney’s Office should be sought on claiming any exemptions.

*Examples include most business documents, minutes of meetings, emails and data related to how Metro services are developed and delivered.*

**c.** **Sensitive** information is defined as information that in isolation may not present any specific risk to the confidentiality, integrity or availability of Metro operations, resources or constituents but if combined with other data could represent inappropriate risk. Sensitive information can be exempt from disclosure under KRS 61.878 or other laws, and the advice of the County Attorney’s Office should be sought on claiming any exemptions.

*Examples include internet protocol (IP) addresses of computer assets, design and procedure documents.*

**d.** **Confidential** information is defined as information that if lost, disclosed, or inappropriately modified could cause significant impact to life safety and/or confidentiality, integrity, availability of Metro operations, resources or constituents.

*Examples include information related to the Metro’s Information Security (aka Cyber Security) controls, strategic planning, operational means and methods, network diagrams, passwords, Card Holder Data (CHD) as defined under PCI, Personal Health Information (PHI), Personally Identifiable Information (PII) and all other legally protected material.*

### 6.2.3 Information and Data Labeling and Handling

All media shall be labeled with its information classification to ensure the proper security controls are placed around the media while handling.

a. Data Owners are responsible for ensuring that all removable media containing *non-Public* data is labeled with its information classification, owner, contact information and purpose. HIPAA: 164.310(d)(1), ISO: 7.2.2, PCI: 12.3.4

b. Technology Operations and Enterprise Network Architecture is responsible for ensuring that efforts are made to separate C*onfidential* information from other information with specific security or control requirements. ISO: 7.2.2

c. All employees and contractors are responsible for ensuring that any electronic information approved for deletion from computer systems and discarded hard copy documents are destroyed in a manner to protect disclosure of the information to external parties commensurate with the information's business value or confidentiality. HIPAA: 164.310(d)(1)(i), ISO: 7.2.2

d. Data Owners or designated Data Custodians are responsible for ensuring that all *Confidential* information is secured in one of the following ways: ISO: 7.2.2

- Hard copy information shall be kept in an access-controlled room which is secured when unoccupied or within locked file cabinets with limited access if a secured room is not available; and
- Electronic information shall be encrypted using a Cybersecurity Office approved method when stored on any portable device or media (e.g., laptop, hard drive, tape, compact disc, flash drive). HIPAA: 164.310(a)(1), ISO: 7.2.2

e. Media Handling
Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. ISO 27001 (A,8.3.1). Media shall be disposed of securely when no longer required, using formal procedures. ISO 27001 (A,8.3.2). Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. ISO 27001 (A,8.3.3)

### 6.2.4 Information and Data Management

To help ensure legal and information security control of all Metro data, all data at rest shall remain within the physical boarders of the United States.

a. Data Owners are responsible to ensure that no Metro owned data is forwarded to non-US locations unless as part of approved business operations which has prior approval from the Cybersecurity Office. NIST 800-53, FedRAMP

b. Data Owners, in partnership with the DoIT, Procurement Services, and the Office of the County Attorney shall ensure that all contracts with third-parties, who may come in contact with Metro data, meet or exceed NIST 800-53 and/or FedRAMP-moderate level security controls.

## Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 01/01/2017 | 1.0 | Initial Draft | CISO |
| 01/08/2019 | 1.1 | Content clarification and edits | CISO |
| 12/7/2021 | 1.2 | Content edits | CISO |
| | | | |
| | | | |
| | | | |
| | | | |