COMMONWEALTH OFFICE OF TECHNOLOGY	Page 1 of 4
Office of the Chief Information Officer Enterprise Policy (CIO)	

CIO–110: Enterprise Data Management Policy		
EFFECTIVE DATE: 02/26/2019	**REVISED:** 10/24/2019, 01/23/2024	**REVIEWED:** 10/24/2019, 02/23/2024

I. PURPOSE

This document establishes policies related to the management and sharing of the Commonwealth's enterprise data resources. The policy provides guidance in decision-making and identifies best practices that encourage sharing, optimize resources, mitigate risk, and maximize return on investment.

II. DEFINITIONS

Terms and concepts utilized throughout this document can be found below and within the ENT-101 (Enterprise Data Classification) and ENT-102 (Enterprise Data Classification Standard Process) policy documents.

"Authoritative Data Source" - means a source of data that is recognized by an appropriate set of governance entities to be valid or trusted due to its reliability, accuracy, or the fact that it originated from an official agency, publication, or other such reference.

"Data Clearinghouse" - means a managed repository of valid or trusted data that is recognized by an appropriate set of governance entities and supports the governance entity's business environment.

"High-Value Data Elements" - means data that can increase agency accountability and responsiveness; improve public knowledge of the agency and its operations thus furthering its core mission; create economic opportunity; or respond to need and demand as identified through public consultation.

"Metadata" - means data that provides information about data. For example, metadata may include definitions of database objects such as fields, base tables, views, synonyms, value ranges, indexes, users, and user groups. Metadata can be thought of as the "pedigree" or "vintage" of a particular dataset.

"Open Data" - means open data is data that can be freely used, re-used, and redistributed by anyone - subject only, at most, to the requirement to attribute and share-a-like.

"Spatial Data" - means Data that is representative of a specific, geographic location on the surface of the Earth. Also known as geospatial data.

III. POLICY

This policy recognizes the Commonwealth's enterprise data resources as an asset and promotes cross-organizational sharing by fostering a collaborative environment that focuses

CIO–110: Enterprise Data Management Policy		
EFFECTIVE DATE: 02/26/2019	**REVISED:** 10/24/2019, 01/23/2024	**REVIEWED:** 10/24/2019, 02/23/2024

on data usability, integrity, availability, interoperability, and security. Adoption and implementation of this policy will maximize the return on investment (ROI) associated with this critical resource.

The establishment of enterprise data resource policies and development of a framework for practice must be a collaborative effort of agency stakeholders based upon the principles outlined below:

a) The Commonwealth's enterprise data resources should be recognized and managed as assets.
b) Data sharing improves data integrity, enhances transparency, reduces duplicative data collection efforts and storage, and maximizes ROI.
c) Adoption and application of enterprise data standards ensure that data assets can be relied upon by multiple business processes.
d) Providing cross-organizational access to enterprise data resources minimizes duplicative storage, enhances business processes, and improves the offerings that the Commonwealth of Kentucky provides.

Roles

The Commonwealth of Technology (COT) and each Executive Branch agency are recognized as peer-level stakeholders in the development, maintenance, and implementation of this enterprise policy and planning document. The role of COT is described below.

Commonwealth Office of Technology

COT will collaborate with agency stakeholders to establish and publish Kentucky-specific enterprise data resource policies and associated, industry-standard best-practices. COT will monitor procurement activities to ensure that data standard requirements are captured in solicitations and contract awards.

a. COT Responsibilities: Facilitate the sharing of data within and between levels of government to enhance business processes, maximize return on investments in data, and promote transparency.
b. Promote effective data governance strategies designed to maintain data integrity, confidentiality, availability, security, and to promote access to data.
c. Encourage open government data efforts including coordinating and managing how the Commonwealth offers interaction with its valuable data resources.
d. Participate in multi-agency information technology projects to ensure data standards are embraced and duplicative efforts are identified and averted.
e. Identify tools and processes for routine sharing of open data with the public and data sharing tools to support cross-organizational sharing and collaboration.

f. Advocate for the sharing of authoritative data sources that have cross-organizational value.

Data Sharing

All open data (i.e., confidential, or internal) should be shared between agencies and with the public when appropriate. Data Sharing Agreements (DSA) are not mandatory for the sharing of data in this category.

Agencies are encouraged to expose data sources for other agencies to consume rather than providing access via extracts, backups, or copies. COT will work with agencies to facilitate these efforts by establishing trusted data pipelines built on a web services framework.

Open Data

By embracing the open data paradigm, Kentucky can begin to maximize its ROI in data resources, employ cost avoidance measures, ensure interoperability, promote transparency, improve efficiencies within business processes, drive innovation, enhance the effectiveness of policies and simplify internal and external discovery of resources.

Confidential Information

The Chief Compliance Officer (CCO) and Chief Information Security Officer (CISO) shall establish a process to maintain confidential data separately and provide access on a need-to-know basis.

When sharing confidential data, agencies shall use a DSA template approved by the Chief Information Officer (CIO), the CCO, and the CISO. Proposed deviations from the approved template for Data Sharing Agreements must be authorized by the CCO prior to execution. Agencies shall submit all data agreements to the CCO for review.

IV. CORRECTIVE OR DISCIPLINARY ACTION

Each agency shall ensure that all relevant staff within their organizational authority are aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy .

CIO–110: Enterprise Data Management Policy		
EFFECTIVE DATE: 02/26/2019	**REVISED:** 10/24/2019, 01/23/2024	**REVIEWED:** 10/24/2019, 02/23/2024

V.   APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy that may have additional information or clarification.

VI.   REFERENCE

Helpful references can be found on the Enterprise IT Policies webpage

ENT-101 (Enterprise Data Classification)

ENT-102 (Enterprise Data Classification Standard Process)