

Office of the Chief Information Officer Enterprise Policy

CIO-110: Enterprise Data Management Policy

Effective Date: 2/26/2019

Last Revised: 10/24/2019

Last Reviewed: 10/24/2019

Policy Statement

This policy establishes controls related to Enterprise Data Management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

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

Metadata: Data that provides information about other data. For example, metadata may include definitions of database objects such as fields, base tables, views, synonyms, value ranges, indexes, users, and user groups.

Policy

The purpose of this policy is to manage Commonwealth data as an asset, focused on maintaining data integrity, confidentiality, availability, and security to maximize its benefit.

The following principles apply to establish data management standards and a framework for practice that safeguard data and maximizes its efficient use:

- Data are business and technical resources that can be managed as assets.
- There are costs associated with the collection, management and protection of data. Every effort should be made to avoid redundant data collection and management activities.
- Data sharing reduces redundant data collection and can improve the reliability of data for multiple users.
- While data should be maintained and managed as close to the data source as possible, data standards must be maintained to ensure the data can be relied upon by multiple users.
- Providing accessibility to data across organizational silos promotes the reduction of data management redundancy, and enhances the services and offerings that the Commonwealth of Kentucky, its agencies, and its partners can provide.

Responsibilities

The Commonwealth's Chief Data Officer (CDO) is responsible for development, implementation, and maintenance of standards and best practices to manage Commonwealth data efficiently and continuously advance the maturity of the data management practice across the Commonwealth's Executive Agencies. The CDO shall coordinate and oversee the sharing of data and shall implement effective data governance strategies designed to maintain data integrity, confidentiality, availability, security, and to promote access to data.

For data sharing, agencies shall use a Data Use Agreement (DUA) template approved by the Chief Information Officer (CIO), the Chief Compliance Officer (CCO), the Chief Information Security Officer (CISO), and the CDO. Any proposed deviations from the approved template for Data Use Agreements need to be authorized by the CDO, CISO, CCO, and CIO prior to execution. Agencies shall submit all data agreements to the CCO for review. After new/revised data agreements are finalized, the CCO shall provide the final agreement to the CDO who will establish and maintain a repository of all Commonwealth data agreements.

Data Stewardship

Chief Data Officer of the Commonwealth (CDO)

The CDO shall ensure that data, information and analytics conform to Commonwealth data management standards. The CDO and the Office of the CDO shall ensure practices and policies are developed and maintained to align with data management best practice.

The CDO is the chief steward of all data within the Commonwealth. The CDO shall establish and publish Commonwealth data standards and associated processes, as appropriate. The CDO shall also support procurement activities to ensure that data standard requirements are captured in solicitations and contract awards.

The Office of the Chief Data Officer shall:

- Develop and maintain an inventory of data sharing agreements and an inventory of data sources and datasets.
- Make the catalog accessible to authorized staff across the Commonwealth agencies. The catalog shall be updated when data sources/datasets are added, modified or removed. The catalog shall be reviewed for accuracy at least once per year.

The CCO and CISO shall establish a process to maintain sensitive information separately and provide access on a need-to-know basis. The CDO shall invoke that process as necessary in support of managing data as an asset.

Agency Data Officer

Executive branch agencies shall designate an Agency Data Officer (ADO) with dual reporting responsibility for all issues related to data management; first, directly to the Agency Head, and second, to the Commonwealth Chief Data Officer (CDO). The ADO shall lead Agency activities in managing data as an asset, leveraging data within and across Commonwealth of Kentucky Agencies, establishing and enforcing data quality and governance, and continuing to advance the state of data management maturity within the Agency.

The ADO will be a senior member of staff with primary responsibility for data management and operations. For large Agencies, the anticipation is that this is a full time role. The responsibilities assigned to this role shall not be further delegated. The ADO will collaborate with Commonwealth Executive Agencies, other Commonwealth Agencies, county and local jurisdictions, education, and not-for-profit organizations as part of the Commonwealth data management initiatives.

Responsibilities of the ADO include but are not limited to:

- Act as a conduit for two-way communication between their Agency and the Office of the CDO ensuring Agency business requirements are communicated to the CDO and data policies and practices are followed by all Agency organizations and personnel;
- Establish and administer a repository of all Agency data agreements, accessible by designated Commonwealth data authority;
- Assist in the development of the Agency data inventory, including identification of high-value data elements and the business applications that rely on them, and shall ensure their Agency supports the continuing maintenance of the inventory;
 - Ensure that all “new” systems or applications submit their data dictionary and data model for review and approval during preliminary system design/configuration. Ensure that systems comply with data sourcing guidelines prior to “go-live”
 - Ensure that all legacy systems or applications undergoing a significant revision have updated data dictionary and data model reviewed and approved during preliminary system design/configuration. Ensure that systems comply with data sourcing guidelines prior to “go-live.”
- Develop and maintain a data source inventory describing and categorizing the data created or collected by the state Agency, including geospatial data used in a state Agency’s Geographic Information System (GIS);
- Develop and maintain an Agency open data catalog, machine-readable open datasets, and oversee the administration of the Agency’s datasets on the Open Data Portal;
- Develop and maintain an inventory of all interfaces that describes inbound or outbound datasets generated, aggregated, stored, purchased, or shared by the state Agency;
- Submit Agency’s data warehousing, data analytics, and data visualization plans to the CDO for approval prior to procurement or execution of such activities. Lead Agency efforts in coordinating such plans with Enterprise data initiatives;
- Enforce Commonwealth’s Enterprise data policies, including but not limited to, Data Management Policy, Data Management Standards, and Data Quality Policies and Standards, within the Agency;
- Lead the advancement of Agency data management maturity;
- Participate in Commonwealth Data Working Group (DWG), DWG subcommittees, and other data initiatives and committees as appropriate;
- Participate in Commonwealth Data Plan activities and lead Agency Data Management planning, including the development of roadmaps and tracking, reporting, and managing roadmap implementation;
- Establish, maintain, and enforce Agency data policies, procedures, and practices.

Data Management Practice

The CDO shall develop and publish a data management framework for use across agencies, including strategies, tools, and practices for data warehousing, data modelling, data integration, data quality, and data analytics.

The Office of the Chief Data Officer shall be the lead organizational entity within the Executive Branch for ensuring data is available, reliable, consistent, accessible, secure, and timely to support the Commonwealth’s mission and activities by:

- Establishing and maintaining enterprise data governance
- Aligning and standardizing data models, and leading the reduction of duplicative data collections
- Managing an open government data effort including coordinating and managing how the Commonwealth offers interaction with Commonwealth data sources
- Creating, managing, and delivering public data products, and developing, establishing, and overseeing methodologies and technologies for delivering and sharing data
- Developing and facilitating strategies for decreasing the cost of data management while increasing the value of Commonwealth data
- Improving how the Commonwealth collects, uses, manages, and publishes data
- Leading Commonwealth efforts to track data collections, data purchases, databases, physical data models, data warehouses, and linkages between datasets
- Improving data quality, developing data quality measurements, and managing the measurement of data quality
- Facilitating the creation and conduct of a Commonwealth Data Working Group which includes Commonwealth agencies, state, regional, and local public entities, and public institutions of higher education. The working group shall implement effective data governance strategies designed to further data sharing, maintain data confidentiality, integrity, availability, security, and promote access to data.

ADOs (and their subordinates) shall collaborate with the Office of the Chief Data Officer in developing practice and standards. As specific strategies and standards are implemented, ADOs shall lead implementation and governance activities within their respective agencies.

Compliance, Monitoring and Review

The Office of the Chief Data Officer and the CCO shall share compliance and monitoring authority for all data management activities. Any exception to policy, standards, or practice shall be resolved at the lowest level practical.

The CDO shall develop and publish a data management exception policy and process.

Open Data Management and Reporting

The CDO shall develop communication strategies to promote and develop business rules, guidelines and practices for data management and sharing within the Commonwealth, to include state, local government, academic institutions, and private interests.

In support of developing public data products and promoting data sharing, the CDO may request reports from, or liaison with external entities, to document available or planned data repositories and to facilitate data sharing. The Chief Data Officer and the Office of the Chief Data Officer will identify tools and processes for routine sharing of “open data” with the public and data sharing tools to support inter-agency (non-“open” data) collaboration.

Cataloged metadata shall be publicly available if there are no information security, sensitivity, or regulatory concerns. Issues precluding the publication of data sources or datasets shall be identified, and conditions for accessing that metadata will be established. Such data will be provided on a need-to-know basis.

The CDO and the Office of the CDO will identify enterprise data management tools for use across agencies and will be responsible for their administration.

Authority

[KRS 42.726](#) authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

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.

Responsibility for Compliance

Each agency shall ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. 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.

Maintenance

COT's Office of Contracts and Privacy is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

References

[KRS 42.726](#), *Roles, duties, and activities of COT*